

Lukas Pottmeyer

Lösungen zu den Aufgaben aus: Diskrete Mathematik

Ein kompakter Einstieg

14. Juni 2019

Springer Nature

Inhaltsverzeichnis

1	Lösungen der Übungsaufgaben	1
1.1	Lösungen der Aufgaben aus Kapitel 1	1
1.2	Lösungen der Aufgaben aus Kapitel 2	7
1.3	Lösungen der Aufgaben aus Kapitel 3	17
1.4	Lösungen der Aufgaben aus Kapitel 4	20
1.5	Lösungen der Aufgaben aus Kapitel 5	26
1.6	Lösungen der Aufgaben aus Kapitel 6	45
1.7	Lösungen der Aufgaben aus Kapitel 7	50
1.8	Lösungen der Aufgaben aus Kapitel 8	54

Kapitel 1

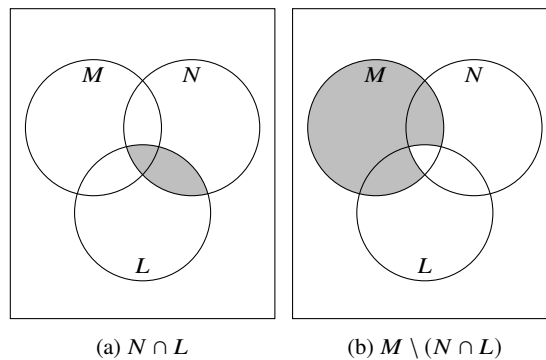
Lösungen der Übungsaufgaben

Hier werden Lösungen zu den Übungsaufgaben vorgestellt. Es gibt oft viele verschiedene (richtige) Lösungswege. Es ist daher sehr gut möglich, dass sich Ihre Lösung zu einer Aufgabe vom hier vorgestellten Lösungsweg unterscheidet. Weiter sind manche Lösungen recht ausführlich geworden und haben den formalen Ansatz des Buches weitergeführt. Damit kann es passieren, dass Ihre Lösungen deutlich kürzer sind als diese hier.

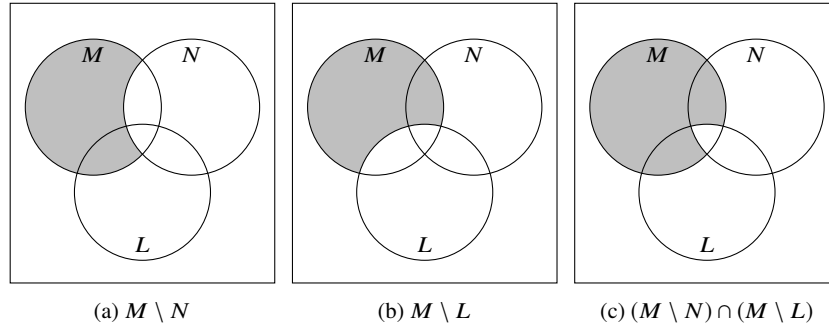
1.1 Lösungen der Aufgaben aus Kapitel 1

Lösung von Aufgabe 1 Seien M, N, L Mengen.

- (a) Wir skizzieren die gesuchten Mengen nacheinander und stellen fest, dass die Skizzen übereinstimmen. Wir haben einerseits



und andererseits



- (b) Es gilt $a \notin N \cap L$, wenn a nicht sowohl in N als auch in L ist. Das bedeutet genau, dass a nicht in N oder nicht in L ist. Damit erhalten wir

$$\begin{aligned}
 a \in M \setminus (N \cap L) &\iff a \in M \text{ und } a \notin N \cap L \\
 &\iff a \in M \text{ und } (a \notin N \text{ oder } a \notin L) \\
 &\iff (a \in M \text{ und } a \notin N) \text{ oder } (a \in M \text{ und } a \notin L) \\
 &\iff (a \in M \setminus N) \text{ oder } (a \in M \setminus L) \\
 &\iff a \in (M \setminus N) \cup (M \setminus L)
 \end{aligned}$$

Das bedeutet, dass die Elemente in $M \setminus (N \cap L)$ genau diejenigen sind, die auch in $(M \setminus N) \cup (M \setminus L)$ liegen. Damit sind die beiden Mengen gleich.

Lösung von Aufgabe 2 (a) *Induktionsanfang:* Für $n = 0$ (das ist die kleinste Zahl für die die Behauptung stimmen soll, also muss dies auch unseren Induktionsanfang darstellen), ist $\sum_{i=0}^n i \cdot (i+1) = \sum_{i=0}^0 i \cdot (i+1) = 0 \cdot (0+1) = 0 = \frac{(0+2) \cdot (0+1) \cdot 0}{3}$. Die Behauptung gilt also für $n = 0$ und der Induktionsanfang ist erledigt.

Induktionsvoraussetzung: Für beliebiges aber festes $n \in \mathbb{N}_0$ gelte $\sum_{i=0}^n i \cdot (i+1) = \frac{(n+2) \cdot (n+1) \cdot n}{3}$.

Induktionsschritt: Sei n wie in der Induktionsvoraussetzung. Wir zeigen, dass die Gleichung auch noch gilt, wenn wir n durch $n+1$ ersetzen. Dies folgt aus

$$\begin{aligned}
 \sum_{i=0}^{n+1} i \cdot (i+1) &= \left(\sum_{i=0}^n i \cdot (i+1) \right) + (n+1) \cdot (n+2) \\
 &\stackrel{IV}{=} \frac{(n+2) \cdot (n+1) \cdot n}{3} + (n+1) \cdot (n+2) \\
 &= (n+2) \cdot (n+1) \cdot \left(\frac{n}{3} + 1 \right) = (n+2) \cdot (n+1) \cdot \frac{n+3}{3} \\
 &= \frac{(n+3) \cdot (n+2) \cdot (n+1)}{3} = \frac{((n+1)+2) \cdot ((n+1)+1) \cdot (n+1)}{3}
 \end{aligned}$$

Im ersten Gleichheitszeichen, haben wir einfach den letzten Summanden in der Summe separat betrachtet. Damit gilt die Formel tatsächlich auch wenn wir überall n durch $n + 1$ ersetzen, und der Induktionsschritt ist ebenfalls beendet. Es folgt, dass für alle $n \in \mathbb{N}_0$ die Gleichung $\sum_{i=0}^n i \cdot (i + 1) = \frac{(n+2) \cdot (n+1) \cdot n}{3}$ gilt.

- (b) Hier muss man zunächst ein bisschen ausprobieren. Wir berechnen die Summen der ersten n ungeraden Zahlen für sehr kleine n :

$$n = 1 : 1$$

$$n = 2 : 1 + 3 = 4$$

$$n = 3 : 1 + 3 + 5 = 9$$

$$n = 4 : 1 + 3 + 5 + 7 = 16$$

$$n = 5 : 1 + 3 + 5 + 7 + 9 = 25$$

Diese Zahlenreihe sollte Ihnen etwas sagen. Es kommt immer eine Quadratzahl raus! Wir vermuten also, dass die Summe der ersten n ungeraden Zahlen gleich n^2 ist.

Wie sieht denn nun die n -te ungerade Zahl aus? Die erste ungerade Zahl ist 1 und wir erhalten die zweite indem wir $1 + 2$ rechnen, die dritte indem wir $1 + 2 + 2$ rechnen und allgemein die n -te indem wir $1 + (n - 1) \cdot 2$ rechnen. Die n -te ungerade Zahl ist also gleich $1 + (n - 1) \cdot 2 = 2n - 1$. Unsere Vermutung können wir nun also formulieren als:

$$\sum_{i=1}^n (2i - 1) = n^2. \quad (1.1)$$

Diese Formel beweisen wir jetzt per Induktion über n .

Induktionsanfang: Jetzt ist die kleinste Zahl für die die Aussage stimmen soll die 1. Wir müssen die Formel also für $n = 1$ überprüfen. In diesem Fall ist die Gleichung offensichtlich, denn es ist $\sum_{i=1}^1 (2i - 1) = 2 - 1 = 1 = 1^2$.

Induktionsvoraussetzung: Für beliebiges aber festes $n \in \mathbb{N}$ gelte $\sum_{i=1}^n (2i - 1) = n^2$.

Induktionsschritt: Sei n wie in der Induktionsvoraussetzung. Wir zeigen, dass 1.1 auch für $n + 1$ gilt (also auch dann, wenn wir jedes n durch ein $n + 1$ ersetzen). Dies können wir ganz direkt überprüfen, in dem wir wie in (a) einfach den letzten Summanden von der Summe abspalten:

$$\sum_{i=1}^{n+1} (2i - 1) = \left(\sum_{i=1}^n (2i - 1) \right) + (2(n + 1) - 1) \stackrel{IV}{=} n^2 + 2n + 1 = (n + 1)^2$$

Das mussten wir zeigen.

Lösung von Aufgabe 3 Der Induktionsschritt funktioniert nicht für $n = 1$ (für alle anderen n wäre das Argument in Ordnung) und somit nicht für ein beliebiges n , wie es in der Induktionsvoraussetzung gefordert wird. Denn für $n = 1$ ist $S' = \{s_1\}$ und

$S'' = \{s_2\}$. Man kann somit nicht schließen, dass es eine Person gibt, die in S' und in S'' ist.

Lösung von Aufgabe 4 Der Beweis ist bereits im Anhang zu Kapitel 1 aufgeführt.

Lösung von Aufgabe 5 Induktionsanfang: Für $n = 6$ (wieder ist dies das kleinste n , für das die Behauptung gelten soll), ist die Aufteilung des Quadrates in sechs kleinere Quadrate bereits in der Aufgabenstellung angegeben.

Induktionsvoraussetzung: Für beliebiges aber festes $n \geq 6$ gelte, dass sich ein Quadrat in k kleinere Quadrate aufteilen lässt, für alle $k \in \{6, \dots, n\}$.

Induktionsschritt: Wir zeigen, dass sich ein Quadrat für das n aus der Induktionsvoraussetzung auch in $n + 1$ kleinere Quadrate aufteilen lässt.

Für $n = 6$ und $n = 7$ haben wir dies bereits in der Aufgabenstellung eingesehen. Wir dürfen also $n \geq 8$ annehmen. Nach Induktionsvoraussetzung lässt sich ein Quadrat somit in $n - 2$ kleinere Quadrate aufteilen. Wir nehmen diese Aufteilung und ersetzen eines der Quadrate durch ein $\begin{smallmatrix} \square & \square \\ \square & \square \end{smallmatrix}$. Da wir ein Quadrat durch vier Quadrate ersetzt haben, erhalten wir eine Aufteilung in $(n - 2) + 3 = n + 1$ Quadrate. Das mussten wir zeigen.

Lösung von Aufgabe 6 Zu (i): Die Abbildung ist nicht injektiv, da $f(0) = 0 = f(1)$. Die Abbildung ist auch nicht surjektiv: Es ist $f(0) = f(1) = 0$ und $f(2) = 2$. Weiter ist $f(n + 1) \geq f(n)$ für alle $n \in \mathbb{N}_0$, da $(n + 1)^2 - (n + 1) = n^2 - n + 2n$ und $2n \in \mathbb{N}_0$ ist. Damit folgt $f(n) \geq f(2) = 2$ für alle $n \geq 2$, was insbesondere $f(n) \neq 1$ für alle $n \in \mathbb{N}_0$ bedeutet. (Das war eine Lösung, die nur die nötigsten Definitionen benutzt. Deutlich eleganter geht es mit ein bisschen Zahlentheorie: $f(n) = n^2 - n = n(n + 1)$ ist immer gerade, da sicher für jedes n entweder n oder $n + 1$ gerade ist.)

Zu (ii): Die Abbildung ist nicht injektiv, da $f(0) = f(2)$. Sie ist surjektiv, da bereits $\{f(0), f(1)\} = \{0, 1\}$.

Zu (iii): Im Beweis von Korollar 1.51 wurde gezeigt, dass diese Abbildung bijektiv ist.

Lösung von Aufgabe 7 Formulieren wir die Aufgabe mit Hilfe der Definition von *gleichmächtig* etwas um, bleibt zu zeigen, dass es eine bijektive Abbildung zwischen $\{n^2 | n \in \mathbb{N}_0\}$ und $\{2n + 1 | n \in \mathbb{N}_0\}$ gibt. Wir gehen dabei einen kleinen Umweg und zeigen, dass beide Mengen gleichmächtig zu \mathbb{N}_0 sind. Eine Abbildung zwischen \mathbb{N}_0 und $\{n^2 | n \in \mathbb{N}_0\}$ drängt sich ja bereits auf. Nämlich

$$f_1 : \mathbb{N}_0 \longrightarrow \{n^2 | n \in \mathbb{N}_0\} \quad ; \quad n \mapsto n^2$$

Offensichtlich ist diese Abbildung surjektiv. Um die Injektivität zu zeigen, nehmen wir $f_1(n) = f_1(k)$ an und folgern daraus $n = k$. Angenommen, es wäre $f_1(n) = f_1(k)$ aber $n \neq k$. Dann ist entweder $n > k$ oder $n < k$. Durch Vertauschen der Rollen von n und k dürfen wir ohne weiteres $n > k$ annehmen, was $n = k + n_0$ bedeutet für ein $n_0 \in \mathbb{N}$. Dann ist aber $n^2 = (k + n_0)^2 = k^2 + 2kn_0 + n_0^2$ und aus $2kn_0 + n_0^2 \neq 0$ folgt $n^2 \neq k^2$. Dies ist ein Widerspruch zu $f_1(n) = f_1(k)$. Es ist also nicht möglich, dass $f_1(n) = f_1(k)$ und $n \neq k$ gilt. Damit muss aus $f_1(n) = f_1(k)$ bereits $n = k$ folgen.

Das bedeutet nichts anderes als dass f_1 injektiv – und somit bijektiv – ist. (Natürlich können Sie auch Ihr Schulwissen über das Wurzelziehen benutzen. Dann folgt aus $f_1(n) = n^2 = k^2 = f_1(k)$ genau $n = \pm k$. Da $n \in \mathbb{N}_0$ liegt, ist ein negatives Vorzeichen nicht möglich und es folgt ebenfalls $n = k$.)

Da f_1 bijektiv ist, gibt es auch eine (bijektive) Umkehrabbildung f_1^{-1} von $\{n^2 | n \in \mathbb{N}_0\}$ nach \mathbb{N}_0 .

Nun zeigen wir, dass auch $\{2n + 1 | n \in \mathbb{N}_0\}$ und \mathbb{N}_0 gleichmächtig sind. Dazu betrachten wir natürlich

$$f_2 : \mathbb{N}_0 \longrightarrow \{2n + 1 | n \in \mathbb{N}_0\} \quad ; \quad n \mapsto 2n + 1$$

Wieder ist die Surjektivität offensichtlich und es ist

$$f_2(n) = f_2(k) \implies 2n + 1 = 2k + 1 \implies 2n = 2k \implies n = k.$$

Damit ist f_2 auch injektiv und somit bijektiv. Wir betrachten die Hintereinanderausführung von f_1^{-1} und f_2 :

$$\{n^2 | n \in \mathbb{N}_0\} \xrightarrow{f_1^{-1}} \mathbb{N}_0 \xrightarrow{f_2} \{2n + 1 | n \in \mathbb{N}_0\}$$

Wir sehen, dass $f_2 \circ f_1^{-1}$ eine Abbildung von $\{n^2 | n \in \mathbb{N}_0\}$ nach $\{2n + 1 | n \in \mathbb{N}_0\}$ ist. Weiter ist $f_2 \circ f_1^{-1}$ eine Hintereinanderausführung von zwei bijektiven Abbildungen und damit selbst bijektiv. Damit sind die Mengen $\{n^2 | n \in \mathbb{N}_0\}$ und $\{2n + 1 | n \in \mathbb{N}_0\}$ also tatsächlich gleichmächtig.

Lösung von Aufgabe 8 Es sind zwei Implikationen zu zeigen.

\Rightarrow Sei also $n \geq k$, mit $n, k \in \mathbb{N}$. Dann ist $\{1, \dots, k\} \subseteq \{1, \dots, n\}$. Wir definieren die Abbildung

$$f : \{1, \dots, n\} \longrightarrow \{1, \dots, k\} \quad ; \quad i \mapsto \begin{cases} i & , \text{ falls } i \leq k \\ 1 & , \text{ falls } i > k \end{cases}$$

Da alle Elemente $1, 2, \dots, k$ im Bild von f liegen, ist diese Abbildung surjektiv.

\Leftarrow Wir beweisen die Aussage per Induktion über k .

Induktionsanfang: $\boxed{k = 1}$ Ist $n \in \mathbb{N}$ beliebig und $f : \{1, \dots, n\} \longrightarrow \{1\}$ eine Abbildung, so ist zwangsläufig $n \geq 1$. (Der Induktionsanfang ist also trivialerweise erfüllt.)

Induktionsvoraussetzung: Für beliebiges aber festes $k \in \mathbb{N}$ gelte: Falls $f : \{1, \dots, n\} \longrightarrow \{1, \dots, k\}$ surjektiv ist, dann ist $n \geq k$.

Induktionsschritt: $\boxed{k \mapsto k + 1}$ Sei also $f : \{1, \dots, n\} \longrightarrow \{1, \dots, k + 1\}$ surjektiv, für ein $n \in \mathbb{N}$. Dann gibt es für jedes $j \in \{1, \dots, k + 1\}$ mindestens ein $i \in \{1, \dots, n\}$ mit $f(i) = j$. Sei A die Menge aller Elemente aus $\{1, \dots, n\}$, die auf $k + 1$ abgebildet werden. D. h.: $A = \{i \in \{1, \dots, n\} | f(i) = k + 1\}$. Wir erhalten die Abbildung

$$f' : \{1, \dots, n\} \setminus A \longrightarrow \{1, \dots, k\} \quad ; \quad i \mapsto f(i)$$

Diese Abbildung ist wohldefiniert, da wir nachdem die Elemente aus A nicht mehr berücksichtigt werden, nur noch Elemente betrachten, die tatsächlich auf ein Element aus $\{1, \dots, k\}$ abgebildet werden. Da f surjektiv ist, ist auch f' surjektiv.

Wir sortieren die Elemente aus $\{1, \dots, n\} \setminus A = \{m_1, \dots, m_r\}$ der Größe nach. D. h.: es ist $m_1 < m_2 < m_3 < \dots < m_r$ für ein gewisses $r \in \mathbb{N}$. Die Abbildung

$$g : \{1, \dots, r\} \longrightarrow \{1, \dots, n\} \setminus A \quad ; \quad i \mapsto m_i$$

ist damit sicher surjektiv. Weiter ist jedes $m_i \geq i$ und somit $n \geq m_r \geq r$. Wäre $r = n$, so müsste $m_i = i$ für alle $i \in \{1, \dots, n\}$ gelten und es wäre $\{1, \dots, n\} \setminus A = \{1, \dots, n\}$, was ein Widerspruch ist, da A nicht leer ist. Somit ist $r < n$ und $f' \circ g$ eine surjektive Abbildung. Per Induktionsvoraussetzung folgt $n > r \geq k$ und somit $n \geq n + 1 \geq k + 1$. Das war zu zeigen.

Bei diesem Beweis haben wir uns auf den Standpunkt gestellt, dass wir das Additionsprinzip noch nicht kennen.

Lösung von Aufgabe 9 Seien M und N nicht-leere endliche Mengen. Dann gibt es eine bijektive Abbildung $g_M : \{1, \dots, |M|\} \longrightarrow M$ und eine bijektive Abbildung $g_N : \{1, \dots, |N|\} \longrightarrow N$.

Ist nun $f : M \longrightarrow N$ eine Abbildung, so ist $g_N^{-1} \circ f \circ g_M$ eine Abbildung von $\{1, \dots, |M|\}$ nach $\{1, \dots, |N|\}$ (da g_N und g_M bijektiv sind, existieren die Umkehrabbildungen auch tatsächlich). Ist f injektiv (bzw. surjektiv), so ist $g_N^{-1} \circ f \circ g_M$ als Hintereinanderausführung von injektiven (bzw. surjektiven) Abbildungen ebenfalls injektiv (bzw. surjektiv).

Ist andererseits $f : \{1, \dots, |M|\} \longrightarrow \{1, \dots, |N|\}$ eine Abbildung, so ist $g_N \circ f \circ g_M^{-1}$ eine Abbildung von M nach N . Genau wie eben impliziert die Injektivität (bzw. Surjektivität) von f auch die Injektivität (bzw. Surjektivität) von $g_N \circ f \circ g_M^{-1}$.

Zusammengenommen existiert also genau dann eine injektive (bzw. surjektive) Abbildung von M nach N , wenn es eine injektive (bzw. surjektive) Abbildung von $\{1, \dots, |M|\}$ nach $\{1, \dots, |N|\}$ gibt. Damit erhalten wir

$$\begin{aligned} |M| \leq |N| &\stackrel{1.33}{\iff} \exists f : \{1, \dots, |M|\} \longrightarrow \{1, \dots, |N|\} \text{ injektiv} \\ &\iff \exists f : M \longrightarrow N \text{ injektiv} \end{aligned}$$

und genauso

$$\begin{aligned} |M| \geq |N| &\stackrel{1.33}{\iff} \exists f : \{1, \dots, |M|\} \longrightarrow \{1, \dots, |N|\} \text{ surjektiv} \\ &\iff \exists f : M \longrightarrow N \text{ surjektiv} \end{aligned}$$

Lösung von Aufgabe 10 Wir möchten die Tupel (i, j) aus der Tabelle der Reihe nach (von links nach rechts und von oben nach unten gelesen) auf die Elemente $1, 2, \dots$ abbilden. Es soll also gelten: $(1, 1)$ wird auf 1 abgebildet, $(1, 2)$ auf 2, ...,

$(1, n-1)$ auf $n-1$ und $(1, n)$ auf n . Dannach wird $(2, 1)$ auf $n+1$ abgebildet, und so weiter, bis $(2, n)$ auf $n+1 = 2n$ abgebildet wird. Insbesondere soll gelten $(f((1, 1)), \dots, f((1, n))) = (1, \dots, n)$, $(f((2, 1)), \dots, f((2, n))) = (n+1, \dots, 2n)$, und allgemein $(f((i, 1)), \dots, f((i, n))) = ((i-1)n+1, \dots, in)$ für alle $i \in \{1, \dots, k\}$.

Die Abbildung $f : \{1, \dots, k\} \times \{1, \dots, n\} \rightarrow \{1, \dots, k \cdot n\}$, definiert durch $f((i, j)) = (i-1)n + j$ erfüllt genau diese Bedingung. Damit ist f bijektiv.

Lösung von Aufgabe 11 Ein Menu bestehend aus Hauptgericht, Beilage und Nachtisch, kann als Element aus

$$\{\text{Hauptgerichte}\} \times \{\text{Beilagen}\} \times \{\text{Nachtische}\}$$

aufgefasst werden. Damit gibt es mit dem Multiplikationsprinzip

$$\begin{aligned} & |\{\text{Hauptgerichte}\} \times \{\text{Beilagen}\} \times \{\text{Nachtische}\}| \\ &= |\{\text{Hauptgerichte}\}| \cdot |\{\text{Beilagen}\}| \cdot |\{\text{Nachtische}\}| \\ &= 5 \cdot 6 \cdot 3 = 90 \end{aligned}$$

verschiedene Menus, bestehend aus Hauptgericht, Beilage und Nachtisch.

Lösung von Aufgabe 12 Im schlimmsten Fall gibt es keine blauen Dächer, so dass es genau 20 blaue Quader gibt (mehr blaue Quader sind nicht möglich, da es insgesamt nur 20 blaue Steine gibt). Die übrigen 5 Quader müssen notgedrungen rot sein.

Hier noch die Erklärung, was das mit dem Inhalt des Kapitels zu tun hat. Sei Q die Menge aller Quader, D die Menge aller Dächer, R die Menge aller roten Steine und B die Menge aller blauen Steine. Uns interessiert die Zahl $|Q \cap R|$. Da es insgesamt nur 40 Steine gibt, ist $|Q \cup R| \leq 40$. Weiter ist $|Q \cup R| = |Q| + |R| - |Q \cap R|$. Damit folgt $|Q \cap R| \geq |Q| + |R| - 40 = 25 + 20 - 40 = 5$.

1.2 Lösungen der Aufgaben aus Kapitel 2

Lösung von Aufgabe 13 (a) Sie ordnen jedem Freund eine der drei Postkarten zu. Damit ist jede Verteilung der Postkarten gegeben durch eine Abbildung von der Menge Ihrer Freunde in die Menge der Postkarten. Es gibt somit genau 3^{12} Verteilungen der Postkarten an Ihre Freunde. (Für jeden Freund können Sie aus drei Postkarten wählen.)

(b) Wir nennen die Postkarten A , B und C . Weiter setzen wir M_A als die Menge aller Verteilungen der Postkarten an Ihre Freunde, bei denen niemand die Postkarte A bekommt. Genauso definieren wir M_B und M_C . Dann ist die gesuchte Anzahl genau $3^{12} - |M_A \cup M_B \cup M_C|$.

Bei allen Verteilungen in M_A haben sie pro Freund nur zwei Möglichkeiten sich für eine Postkarte zu entscheiden. Damit gilt $|M_A| = 2^{12}$. Genauso erhalten wir auch $|M_B| = |M_C| = 2^{12}$. In der Menge $M_A \cap M_B$ sind genau die Verteilungen, in denen weder A noch B verschickt wird. Es bleibt also für alle Freunde nur

noch Postkarte C übrig und somit gilt $|M_A \cap M_B| = |M_A \cap M_C| = |M_B \cap M_C| = 1$. Der Schnitt aller drei Mengen M_A, M_B, M_C ist natürlich leer. Mit Inklusion-Exklusion erhalten wir nun

$$\begin{aligned} & 3^{12} - |M_A \cup M_B \cup M_C| \\ &= 3^{12} - (|M_A| + |M_B| + |M_C| - |M_A \cap M_B| - |M_A \cap M_C| - |M_B \cap M_C|) \\ &= 3^{12} - 3 \cdot 2^{12} + 3 \end{aligned}$$

Lösung von Aufgabe 14 (a) Gesucht ist die Anzahl von Permutationen von 18 Elementen – also $18!$. (Für den ersten Platz haben wir 18 Möglichkeiten, für den zweiten Platz 17, ...)

- (b) Gesucht ist die Anzahl von 6-Permutationen von 18 Elementen – also $\frac{18!}{12!}$.
- (c) Ist Team C auf dem letzten Platz, so können wir die restlichen 17 Mannschaften auf 17 Plätze verteilen. Es gibt also genau $17!$ Tabellenkonstellationen mit Mannschaft C auf dem letzten Platz. Von diesen Tabellenkonstellationen gibt es genau so viele mit „ A steht vor B “, wie es welche gibt mit „ B steht vor A “ (wir können die Positionen dieser beiden Mannschaften ja einfach vertauschen). Damit gibt es genau $\frac{17!}{2}$ Tabellenkonstellationen mit C steht auf dem letzten Platz und A steht vor B . Da das gleiche gilt natürlich, wenn C auf dem vorletzten Platz steht und genauso, wenn C auf dem letzten Platz steht. Damit gibt es insgesamt $3 \cdot \frac{17!}{2}$ Tabellenkonstellationen mit den gewünschten Eigenschaften.
- (d) Wählen Sie sechs beliebige Mannschaften A, B, C, D, E, F aus. Dann gibt es genau $6! \cdot 12!$ Tabellenkonstellationen in denen die ersten sechs Plätze von den Mannschaften A, B, C, D, E, F belegt werden.

Lösung von Aufgabe 15 Es gibt genau $\frac{4!}{2!} = 12$ Anagramme von *Ohio*, $\frac{6!}{2! \cdot 2!} = 6 \cdot 5 \cdot 3 \cdot 2 = 18 \cdot 10 = 180$ Anagramme von *Kansas* und $\frac{11!}{4! \cdot 4! \cdot 2!} = 34650$ Anagramme von *Mississippi*.

Lösung von Aufgabe 16 Seien also $m, n, k \in \mathbb{N}_0$, mit $k \leq m \leq n$. Wir überprüfen die Formel zunächst rechnerisch. Es ist

$$\binom{n}{m} \cdot \binom{m}{k} = \frac{n!}{m! \cdot (n-m)!} \cdot \frac{m!}{k! \cdot (m-k)!} = \frac{n!}{(n-m)! \cdot k! \cdot (m-k)!}. \quad (1.2)$$

Für das letzte Gleichheitszeichen haben wir lediglich den Faktor $m!$ aus dem Zähler und dem Nenner gekürzt. Genauso erhalten wir auch

$$\binom{n}{k} \cdot \binom{n-k}{m-k} = \frac{n!}{k! \cdot (n-k)!} \cdot \frac{(n-k)!}{(m-k)! \cdot (n-k-(m-k))!} = \frac{n!}{k! \cdot (m-k)! \cdot (n-m)!}. \quad (1.3)$$

Aus den Gleichungen (1.2) und (1.3) lesen wir sofort die gewünschte Gleichung $\binom{n}{m} \cdot \binom{m}{k} = \binom{n}{k} \cdot \binom{n-k}{m-k}$ ab.

Wir geben jetzt eine etwas anschaulichere Lösung, die nur die Definition von Binomialkoeffizienten benutzt (also, dass $\binom{n}{k}$ die Anzahl von k -elementigen Teilmengen einer Menge mit n Elementen ist). Dazu überlegen wir uns wie viele Möglichkeiten

es gibt die Menge $\{1, \dots, n\}$ in drei disjunkte Teilmengen A, B, C zu unterteilen mit $|A| = k$, $|B| = m - k$ und $|C| = n - m$.

Für die Wahl von A haben wir per Definition genau $\binom{n}{k}$ Möglichkeiten. Die Menge B muss nun eine $(m - k)$ -elementige Teilmenge von $\{1, \dots, n\} \setminus A$ sein. Wir haben also noch $\binom{n-k}{m-k}$ Wahlmöglichkeiten. Damit ist dann die Menge C eindeutig durch $\{1, \dots, n\} \setminus (A \cup B)$ bestimmt. Für die Unterteilung in Teilmengen mit den angegebenen Kardinalitäten gibt es also genau $\binom{n}{k} \cdot \binom{n-k}{m-k}$ Möglichkeiten.

Wir berechnen die Anzahl der Unterteilungen nochmal anders. Dazu wählen wir zunächst eine Teilmenge C' von $\{1, \dots, n\}$ mit m Elementen, wofür wir $\binom{n}{m}$ Möglichkeiten haben. Dann wählen wir eine k -elementige Teilmenge A von C' . Dafür haben wir $\binom{m}{k}$ Möglichkeiten. Als letztes setzen wir $B = C' \setminus A$ und $C = \{1, \dots, n\} \setminus C'$, wofür es natürlich keine Wahlmöglichkeiten mehr gibt. Es gibt also genau $\binom{n}{m} \cdot \binom{m}{k}$ Unterteilungen von $\{1, \dots, n\}$ in drei disjunkte Mengen mit den vorgeschriebenen Kardinalitäten.

Da beide Argumentationen richtig sind, folgt wieder $\binom{n}{k} \cdot \binom{m}{k} = \binom{n}{k} \cdot \binom{n-k}{m-k}$.

Falls Sie das nicht anschaulich finden, dann denken Sie sich irgendeinen Kontext dazu aus. Zum Beispiel: Sie haben einen Zaun aus n weißen Latten. Diesen wollen Sie so anmalen, dass er am Ende aus k schwarzen, $m - k$ grünen und $n - m$ weißen Latten besteht. Sie können nun k Latten schwarz anstreichen ($\binom{n}{k}$ Möglichkeiten) und von den restlichen $n - k$ Latten, streichen Sie $m - k$ grün an ($\binom{n-k}{m-k}$ Möglichkeiten). Sie könnten aber auch erstmal m Latten grün streichen ($\binom{n}{m}$ Möglichkeiten) und dann von diesen m grünen nochmal k mit schwarz überstreichen ($\binom{m}{k}$ Möglichkeiten).

Lösung von Aufgabe 17 (a) Jeder kürzeste Weg besteht aus acht Streckenabschnitten, von denen vier nach rechts und vier nach unten führen. Damit gibt es $\binom{8!}{4! \cdot 4!} = \binom{8}{4} = 70$ solcher Wege. (Wir müssen vier der acht Streckenabschnitte auswählen, die nach unten führen sollen).

(b) Wir zählen zunächst wie viele Wege es von A nach B gibt. Das sind genau $3 = \binom{3}{1}$, da wir einen von drei Streckenabschnitten auswählen müssen, der nach unten führt. Genauso gibt es $\binom{5}{3}$ Wege von B nach C. Da wir jeden Weg von A nach B mit jedem Weg von B nach C kombinieren können um einen Weg von A nach C zu erhalten, der über B führt, gibt es genau $\binom{3}{1} \cdot \binom{5}{3} = 30$ solcher Wege. Von den Wegen, die nicht über B führen, gibt es nach Teil (a) also genau $\binom{8}{4} - \binom{3}{1} \cdot \binom{5}{3} = 40$.

Lösung von Aufgabe 18 (a) Es gibt 16 Figuren, die auf 16 Felder verteilen werden sollen. Wenn alle Figuren unterschiedlich wären, gäbe es $16!$ Möglichkeiten dafür. Jedoch können die 8 Bauern, 2 Türme, 2 Springer und 2 Läufer jeweils nicht unterschieden werden. Gleiche Figuren dürfen also beliebig untereinander die Plätze tauschen. Es folgt, dass es genau

$$\frac{16!}{8! \cdot 2! \cdot 2! \cdot 2!}$$

Verteilungen der Figuren auf die ersten zwei Reihen gibt.

(b) Nun wählen wir in einem ersten Schritt 16 Felder aus – wofür es genau $\binom{64}{16}$ Möglichkeiten gibt. In einem zweiten Schritt verteilen wir die 16 Figuren auf

die 16 ausgewählten Felder, wie in (a). Damit gibt es genau

$$\binom{64}{16} \cdot \frac{16!}{8! \cdot 2! \cdot 2! \cdot 2!}$$

Verteilungen der Figuren auf dem gesamten Schachbrett.

Alternativ können wir in Teil (b) auch die 48 leeren Felder (die wir natürlich auch nicht unterscheiden können) mit verteilen. Dann erhalten wir $\frac{64!}{48! \cdot 8! \cdot 2! \cdot 2! \cdot 2!}$ Verteilungen, was das gleiche ist wie unser Ergebnis von oben.

Lösung von Aufgabe 19 Konstruieren Sie einfach alle diese Pokerhände!

- (1) Wähle eine Farbe aus: 4 Möglichkeiten
- (2) Wähle 5 Werte dieser Farbe aus: $\binom{13}{5}$ Möglichkeiten

Das macht zusammen $4 \cdot \binom{13}{5}$ Möglichkeiten eine Pokerhand zu konstruieren, in der alle Karten die gleiche Farbe haben. Natürlich, sind alle diese Pokerhände unterschiedlich. Es gibt also genau $4 \cdot \binom{13}{5}$ dieser Pokerhände.

Lösung von Aufgabe 20 Wir stellen die Studierenden in einer Reihe auf. Dann liefert jede Anordnung der Noten eine andere Verteilung der Noten an die Studierenden, in dem der i -te Studierende in der Reihe, die Note im i -ten Eintrag bekommt. Es gibt also genau

$$\frac{250!}{10! \cdot 10! \cdot 15! \cdot 15! \cdot 25! \cdot 25! \cdot 35! \cdot 35! \cdot 40! \cdot 40!}$$

verschiedene Notenverteilungen.

Lösung von Aufgabe 21 Wir wählen 10-mal eines der drei Kinder aus, das ein Bonbon bekommt. Natürlich ist dabei Wiederholung erlaubt (sogar erforderlich). Die Reihenfolge spielt aber keine Rolle, da es nur darum geht, wie viele Bonbons jedes einzelne Kind am Ende der Verteilung hat. Damit gibt es genau $\binom{10+3-1}{3} = \binom{12}{3} = 220$ Verteilungen der Bonbons.

Wenn jedes Kind mindestens ein Bonbon bekommen soll, dann bekommt vorab jedes Kind ein Bonbon. Die restlichen 7 Bonbons werden dann verteilt wie in (a), wofür es genau $\binom{7+3-1}{3} = \binom{9}{3} = 84$ Möglichkeiten gibt.

Wenn Lea Geburtstag hat und mindestens vier Bonbons bekommen soll, dann machen wir es genauso. Lea bekommt 4 Bonbons und die restlichen 6 Bonbons können auf $\binom{6+3-1}{3} = \binom{8}{3} = 56$ Arten auf alle drei verteilt werden.

Lösung von Aufgabe 22 Sei eine Menge M mit $n \in \mathbb{N}$ Elementen gegeben. Per Definition ist die Anzahl von k -elementigen Teilmengen von M gegeben durch $\binom{n}{k}$. Die Aussage folgt nun aus $\sum_{i=0}^n (-1)^i \binom{n}{i} = 0$ (Korollar 2.27). Denn dies ist äquivalent zu

$$\sum_{\{i \in \{0, \dots, n\} \mid i \text{ ist gerade}\}} \binom{n}{i} = \sum_{\{i \in \{0, \dots, n\} \mid i \text{ ist ungerade}\}} \binom{n}{i}.$$

Auf der linken Seite steht genau die Anzahl aller Teilmengen von M mit einer geraden Anzahl von Elementen und auf der rechten Seite steht die Anzahl von allen

Teilmengen von M mit einer ungeraden Anzahl von Elementen. Diese Gleichheit war also zu zeigen.

Lösung von Aufgabe 23 Mit dem Binomialsatz ist

$$\begin{aligned} (1 + \sqrt{3})^n + (1 - \sqrt{3})^n &= \left(\sum_{i=0}^n \binom{n}{i} \cdot (\sqrt{3})^i \right) + \left(\sum_{i=0}^n \binom{n}{i} \cdot (-\sqrt{3})^i \right) \\ &= \left(\sum_{i=0}^n \binom{n}{i} \cdot (\sqrt{3})^i \right) + \left(\sum_{i=0}^n \binom{n}{i} \cdot (\sqrt{3})^i \cdot (-1)^i \right) \\ &= \sum_{i=0}^n \binom{n}{i} \cdot (\sqrt{3})^i \cdot (1 + (-1)^i) \end{aligned}$$

Der Term $(1 + (-1)^i)$ ist gleich 0, falls i ungerade ist. Es bleiben in der Summe also nur die Summanden mit geradem i übrig. Für gerades i ist aber jeder dieser Summanden in \mathbb{N}_0 . Damit muss die ganze Summe – und somit $(1 + \sqrt{3})^n + (1 - \sqrt{3})^n$ – in \mathbb{N}_0 liegen.

Lösung von Aufgabe 24 Genau wie in Beispiel 2.44 gibt es ohne jede Einschränkung $\binom{5+6-1}{5} = 252$ mögliche Ergebnisse (es werden mit Wiederholung ohne Beachtung der Reihenfolge 5 Werte aus den 6 möglichen Augenzahlen gewählt).

- (a) Wir stellen einen Würfel so auf, dass er eine \boxtimes anzeigt. Dann bleiben noch vier Würfel übrig von denen keiner mehr ein \boxtimes zeigen darf. Es gibt also noch genau $\binom{4+5-1}{4} = 70$ Möglichkeiten die restlichen vier Augenzahlen zu wählen.
- (b) Hier haben wir immer noch fünf Würfel, aber eine Augenzahl weniger, da die \boxtimes nicht angezeigt werden darf. Die gesuchte Anzahl berechnen wir nun wie immer mit $\binom{5+5-1}{5} = 126$.
- (c) Wir haben nur fünf Würfel, die offensichtlich nicht sechs verschiedene Augenzahlen anzeigen können. Es gibt also Null Ergebnisse, die diese Eigenschaft haben.
- (d) Sind alle Augenzahlen verschieden, so wird genau eine Augenzahl nicht angezeigt. Es gibt also genau 6 solcher Ergebnisse.
- (e) Für die Augenzahl, die dreimal angezeigt wird, gibt es 6 Möglichkeiten. Für die Augenzahl, die zweimal angezeigt wird, bleiben dann noch 5 Möglichkeiten. Das macht zusammen $6 \cdot 5 = 30$ verschiedene Full-House.

Lösung von Aufgabe 25 (a) Wir dürfen also keine zwei Steine auf das selbe Feld legen. Wenn wir nun fünf gleiche Steine auf das Schachbrett legen, haben wir nichts anderes gemacht als fünf der 64 Felder auszuwählen. Dafür gibt es genau $\binom{64}{5}$ Möglichkeiten.

Wenn alle Steine eine andere Farbe haben – sagen wir gelb, grün, rot, blau und orange – dann haben wir

- 64 Möglichkeiten den gelben Stein auf das Brett zu legen,
- dannach noch 63 Möglichkeiten den grünen Stein auf das Brett zu legen,

- dannach noch 62 Möglichkeiten den roten Stein auf das Brett zu legen,
- dannach noch 61 Möglichkeiten den blauen Stein auf das Brett zu legen,
- dannach noch 60 Möglichkeiten den orangenen Stein auf das Brett zu legen.

Das macht zusammen $\frac{60!}{(60-5)!}$ Möglichkeiten, die Steine auf dem Brett zu verteilen.

- (b) Ab jetzt dürfen wir die Steine auch stapeln. Um die nicht unterscheidbaren Steine auf das Brett zu verteilen müssen wir also wieder fünf der 64 Felder auswählen, wobei wir ein Feld auch mehrfach wählen dürfen. Dafür gibt es genau $\binom{64+5-1}{5}$ Möglichkeiten. (Alternativ: Die Anzahl der Möglichkeiten ist nur dadurch bestimmt, wie viele Steine auf jedem einzelnen Feld liegen. Ist also x_i die Anzahl von Steinen auf dem i -ten Feld, so muss gelten $\sum_{i=1}^{64} x_i = 5$ und jedes x_i ist in \mathbb{N}_0 . Die Anzahl der Lösungen dieser Gleichung ist $\binom{64+5-1}{5}$.) Haben nun alle Steine eine andere Farbe (wir nehmen die selben Farben wie in (a), so gibt es wieder 64 Möglichkeiten den gelben Stein auf das Feld zu legen. Allerdings wird dadurch nicht die Anzahl von Möglichkeiten die anderen Steine zu positionieren eingeschränkt. Für jeden Stein gibt es also 64 Möglichkeiten. Bei fünf Steinen macht das insgesamt 64^5 Möglichkeiten.

Dieses Beispiel entspricht also genau den bekannten vier Wahlmöglichkeiten von 5 aus 64 Elementen, jenachdem ob die Reihenfolge beachtet wird oder nicht, und ob Wiederholung erlaubt ist oder nicht.

Lösung von Aufgabe 26 Sie wählen aus 10 Elementen (den Eissorten) 4 Elemente (Eiskugeln) aus, wobei die Reihenfolge nicht beachtet wird (uns interessieren nur welche Kugeln im Eisbecher landen) und Wiederholung erlaubt ist. Damit haben Sie $\binom{10+4-1}{4} = \binom{13}{4} = 715$ Möglichkeiten sich einen Eisbecher mit genau 4 Kugeln zusammenzustellen.

Lösung von Aufgabe 27 Wir definieren

$$g : N \longrightarrow M \quad ; \quad (x, y, z) \mapsto (x + 10, y + 2, z + 4).$$

Es gilt $x + y + z = 4$ und somit auch $(x + 10) + (y + 2) + (z + 4) = 4 + 16 = 20$. Aus $x, y, z \in \mathbb{N}_0$ folgt auch sofort $x + 10 \geq 10$, $y + 2 \geq 2$ und $z + 4 \geq 4$. Damit ist g wohldefiniert. Weiter besitzt g die Umkehrabbildung

$$g^{-1} : M \longrightarrow N \quad ; \quad (x', y', z') \mapsto (x' - 10, y' - 2, z' - 4)$$

und ist somit bijektiv.

Genauso definieren wir

$$h : N \longrightarrow L \quad ; \quad (x, y, z) \mapsto (x + 1, y + 3, z).$$

Genau wie gerade sehen wir, dass h wohldefiniert ist, und die Umkehrabbildung

$$h^{-1} : L \longrightarrow N \quad ; \quad (\tilde{x}, \tilde{y}, \tilde{z}) \mapsto (\tilde{x} - 1, \tilde{y} - 3, \tilde{z})$$

besitzt. Damit ist h eine bijektive Abbildung.

Wir können die Abbildung wieder genauso konstruieren wie eben. Wir benutzen aber lieber, dass die Hintereinanderausführung von bijektiven Abbildungen eine bijektive Abbildung ist. Damit ist $f = h \circ g^{-1}$ eine bijektive Abbildung von M nach L und es gilt

$$\begin{aligned} f(x', y', z') &= h(g^{-1}(x', y', z')) = h(x' - 10, y' - 2, z' - 4) \\ &= (x' - 10 + 1, y' - 4 + 3, z' - 4) = (x' - 9, y' - 1, z' - 4). \end{aligned}$$

Lösung von Aufgabe 28 Sei K die Menge der Studierenden, die Käsespätzle auf ihrem Tablett haben, B die Menge der Studierenden, die einen Beilagensalat auf ihrem Tablett haben und V die Menge der Studierenden, die Vanillepudding auf ihrem Tablett haben. Dann ist $K \cup B \cup V$ die Menge von Studierenden, die mindestens eine der Komponenten Käsespätzle, Beilagensalat oder Vanillepudding gewählt haben. Wir suchen also $|K \cup B \cup V|$. Dafür benutzen wir die Inklusions-Exklusions-Formel:

$$|K \cup B \cup V| = |K| + |B| + |V| - |K \cap B| - |K \cap V| - |B \cap V| + |K \cap B \cap V|$$

Alle auftretenden Kardinalitäten sind explizit in der Aufgabenstellung angegeben! Wir setzen diese Kardinalitäten ein und erhalten

$$|K \cup B \cup V| = 21 + 16 + 8 - 12 - 5 - 3 + 2 = 27$$

Lösung von Aufgabe 29 Beim Wichteln wird also jeder Person genau eine andere Person zugeordnet. Damit ist eine solche Auslosung nichts anderes als eine bijektive Abbildung von der Menge der teilnehmenden Personen in sich selbst. Insbesondere gibt es genau $n!$ solcher Auslosungen, wenn n Personen zusammen wichteln.

- (a) Es wichteln die fünf Personen A_1, A_2, A_3, A_4 und A_5 zusammen. Für jedes $i \in \{1, \dots, 5\}$ sei M_i die Menge aller Auslosungen, bei denen A_i sich selbst beschenken soll. Dann ist $\bigcup_{i=1}^5 M_i$ die Menge aller Auslosungen in denen mindestens eine Person sich selbst beschenkt. Nach der Vorbemerkung gibt es also genau

$$5! - |M_1 \cup M_2 \cup M_3 \cup M_4 \cup M_5| \quad (1.4)$$

Auslosungen bei denen niemand sich selbst beschenken muss. Dies berechnen wir natürlich mit Hilfe der Inklusions-Exklusions-Formel. Wenn sich eine fest gewählte Person selbst beschenken soll, können die restlichen vier Personen noch beliebig zugeordnet werden. Es gilt also $|M_i| = 4!$ für alle $i \in \{1, \dots, 5\}$. Allgemein gilt: sollen n fest gewählte Personen jeweils sich selbst beschenken, so können die restlichen $5 - n$ Personen untereinander beliebig zugeordnet werden. Es gibt also $(5 - n)!$ Auslosungen in denen sich n fest gewählte Personen selbst beschenken müssen. Weiter gibt es genau $\binom{5}{n}$ Möglichkeiten n der 5 Personen auszuwählen, die sich selbst beschenken müssen. Mit (1.4) und Inklusion-Exklusion ist die gesuchte Zahl also gleich

$$\begin{aligned}
& 5! - \binom{5}{5} \cdot 4! + \binom{5}{2} \cdot 3! - \binom{5}{3} \cdot 2! + \binom{5}{4} \cdot 1! - \binom{5}{5} \cdot 0! \\
&= 5! - 5! + \frac{5!}{2!} - \frac{5!}{3!} + \frac{5!}{4!} - 1 \\
&= 60 - 20 + 5 - 1 = 44
\end{aligned}$$

(Zusatzaufgabe: In dieser Rechnung hat sich eine ziemlich gute Annäherung an die Eulersche-Zahl e versteckt. Finden Sie diese!)

- (b) Wie zu Beginn bemerkt ist eine Auslosung beim Wichteln zwischen n Personen nichts anderes als eine bijektive Abbildung von einer Menge mit n Elementen nach sich selbst. Die Anzahl von Personen, die sich dabei selbst beschenken müssen ist nichts anderes als die Anzahl von Fixpunkten der zugehörigen bijektiven Abbildung. Der Erwartungswert für die Anzahl von Fixpunkten – und somit der Anzahl von Personen, die sich selbst beschenken müssen – ist gleich 1, was in Beispiel 2.55 berechnet wurde.

Lösung von Aufgabe 30 Sei (Ω, p) ein endlicher Wahrscheinlichkeitsraum und $A, B \subseteq \Omega$.

- (a) Wir rechnen die Wahrscheinlichkeit einfach aus:

$$p[\Omega \setminus A] = \sum_{\omega \in \Omega \setminus A} p(\omega) = \sum_{\omega \in \Omega} p(\omega) - \sum_{\omega \in A} p(\omega) = 1 - p[A]$$

- (b) Das ist eine Umformulierung des einfachsten Falles der Inklusions-Exklusions-Formel. Wir wissen bereits, dass $A \cup B = (A \setminus (A \cap B)) \cup (B \setminus (A \cap B)) \cup ((A \cap B))$ ist, und dass die drei Mengen auf der rechten Seite paarweise disjunkt sind. Damit folgt

$$\begin{aligned}
p[A \cup B] &= \sum_{\omega \in A \cup B} p(\omega) = \sum_{\omega \in A \setminus (A \cap B)} p(\omega) + \sum_{\omega \in B \setminus (A \cap B)} p(\omega) + \sum_{\omega \in A \cap B} p(\omega) \\
&= \sum_{\omega \in A} p(\omega) - \sum_{\omega \in A \cap B} p(\omega) + \sum_{\omega \in B} p(\omega) - \sum_{\omega \in A \cap B} p(\omega) + \sum_{\omega \in A \cap B} p(\omega) \\
&= \sum_{\omega \in A} p(\omega) + \sum_{\omega \in B} p(\omega) - \sum_{\omega \in A \cap B} p(\omega) \\
&= p[A] + p[B] - p[A \cap B]
\end{aligned}$$

- (c) Sei nun p die Gleichverteilung, $|\Omega|$ eine Primzahl und A, B seien weder die leere Menge noch Ω . Wir müssen zeigen, dass A und B *nicht* unabhängig sind. Angenommen A und B wären unabhängig. Dann ist per Definition $p[A \cap B] = p[A] \cdot p[B]$. Da p die Gleichverteilung ist, ist das gleichbedeutend mit $\frac{|A \cap B|}{|\Omega|} = \frac{|A|}{|\Omega|} \cdot \frac{|B|}{|\Omega|}$. Das wiederum bedeutet

$$|\Omega| \cdot |A \cap B| = |A| \cdot |B|.$$

Es ist $|\Omega|$ eine Primzahl und somit muss $|\Omega|$ eine der Zahlen $|A|$ und $|B|$ teilen. Nach Voraussetzung ist aber $|A|, |B| \in \{1, \dots, |\Omega| - 1\}$ und somit ist keine der Zahlen durch $|\Omega|$ teilbar. Das ist ein Widerspruch. Damit muss unsere Annahme, dass A und B unabhängig sind, falsch gewesen sein. Das heißt nichts anderes, als dass A und B nicht unabhängig sind.

Lösung von Aufgabe 31 Diese Aussage wurde für $k = 2$ bereits bewiesen. Für beliebiges k aus \mathbb{N} beweisen wir die Aussage per Induktion.

Induktionsanfang: Für $k = 1$ ist $\omega \mapsto p(\omega)$ per Definition eine Verteilung auf Ω_1 . Der Induktionsanfang ist also trivialerweise erfüllt.

Induktionsvoraussetzung: Für beliebiges aber festes $k \in \mathbb{N}$ sei für je k endliche Wahrscheinlichkeitsräume $(\Omega_1, p_1), \dots, (\Omega_k, p_k)$ die Abbildung $(\omega_1, \dots, \omega_k) \mapsto p_1(\omega_1) \cdot \dots \cdot p_k(\omega_k)$ eine Verteilung auf $\Omega_1 \times \dots \times \Omega_k$.

Induktionsschritt: Sei nun k wie in der Induktionsvoraussetzung und seien $k + 1$ endliche Wahrscheinlichkeitsräume $(\Omega_1, p_1), \dots, (\Omega_{k+1}, p_{k+1})$ gegeben. Nach Voraussetzung ist

$$p : \Omega_1 \times \dots \times \Omega_k \longrightarrow [0, 1] \quad ; \quad (\omega_1, \dots, \omega_k) \mapsto p_1(\omega_1) \cdot \dots \cdot p_k(\omega_k)$$

eine Verteilung auf $\Omega_1 \times \dots \times \Omega_k$. Es ist also $(\Omega_1 \times \dots \times \Omega_k, p)$ ein endlicher Wahrscheinlichkeitsraum. Da die Behauptung für zwei Wahrscheinlichkeitsräume gilt, ist

$$\begin{aligned} ((\omega_1, \dots, \omega_k), \omega_{k+1}) &\mapsto p((\omega_1, \dots, \omega_k)) \cdot p_{k+1}(\omega_{k+1}) \\ &= p_1(\omega_1) \cdot \dots \cdot p_k(\omega_k) \cdot p_{k+1}(\omega_{k+1}) \end{aligned}$$

eine Verteilung auf

$$(\Omega_1 \times \dots \times \Omega_k) \times \Omega_{k+1} = \Omega_1 \times \dots \times \Omega_k \times \Omega_{k+1}.$$

Damit ist die Aussage bewiesen.

Lösung von Aufgabe 32 (a) Wir konzentrieren uns zunächst nur auf die sechs Lottozahlen. Da die Reihenfolge der gezogenen Zahlen keine Rolle spielt, wird in jeder Ziehung eine 6-elementige Teilmenge von $\{1, \dots, 49\}$ gezogen. Wir setzen also $\Omega_L = \{A \in \{1, \dots, 49\} \mid |A| = 6\}$. Da jede der Lottozahlen mit einer gleichen Wahrscheinlichkeit gezogen wird, ist die Verteilung auf Ω_L die Gleichverteilung – nennen wir sie p_L .

Bei der Superzahl wird eine Ziffer aus $\{0, \dots, 9\}$ gezogen, wobei jede Ziffer mit gleicher Wahrscheinlichkeit gezogen werden soll. Der zugehörige Wahrscheinlichkeitsraum für die Ziehung der Superzahl ist also (Ω_S, p_S) mit $\Omega_S = \{0, \dots, 9\}$ und der Gleichverteilung p_S .

Die Ziehung der sechs Lottozahlen, soll natürlich nicht die Ziehung der Superzahl beeinflussen. Die Ausgänge sollen also unabhängig von einander sein. Der Wahrscheinlichkeitsraum für die Lottoziehung ist also der Produktraum

$$(\Omega, p) = (\Omega_L, p_L) \times (\Omega_S, p_S) = (\{A \in \{1, \dots, 49\} \mid |A| = 6\} \times \{0, \dots, 9\}, p),$$

mit der Gleichverteilung p .

- (b) Wir übernehmen die Bezeichnungen aus Teil (a). Ihr abgegebener Tipp sei $(L, s) \in \Omega$. Da wir auf Ω die Gleichverteilung haben, ist die gesuchte Wahrscheinlichkeit gleich

$$\frac{|\{(A, a) \in \Omega \mid |A \cap L| = 2 \text{ und } a = s\}|}{|\Omega|}.$$

Nach der Definition des Binomialkoeffizienten ist $|\Omega| = |\Omega_L| \cdot |\Omega_S| = \binom{49}{6} \cdot 10$. Weiter ist offensichtlich $|\{(A, a) \in \Omega \mid |A \cap L| = 2 \text{ und } a = s\}| = |\{A \in \Omega_L \mid |A \cap L| = 2\}|$. Wir konstruieren einfach alle Elemente A in dieser letzten Menge: Dazu wählen wir zunächst 2 Elemente aus L aus $\binom{6}{2}$ Möglichkeiten und dann wählen wir die restlichen 4 Elemente aus $\{1, \dots, 49\} \setminus L$ aus $\binom{43}{4}$ Möglichkeiten. Es gibt also $\binom{6}{2} \cdot \binom{43}{4}$ Elemente $A \in \Omega_L$ mit $|A \cap L| = 2$. Setzen wir alles zusammen erhalten wir, dass die gesuchte Wahrscheinlichkeit gleich

$$\frac{\binom{6}{2} \cdot \binom{43}{4}}{\binom{49}{6} \cdot 10} = \frac{1851150}{139838160} = 0,013237 \dots$$

ist.

Lösung von Aufgabe 33 Die Karten eines Kartenspieles mit 52 Karten lassen sich in $52!$ unterschiedlichen Reihenfolgen übereinander stapeln (jeder Stapel entspricht einer Permutation der Karten). Dass das Kartenspiel gründlich gemischt wird, soll dazu führen, dass jeder der möglichen Stapel mit einer gleichen Wahrscheinlichkeit auftritt. Wir betrachten also die Gleichverteilung p auf der Menge aller Kartestapel.

- (a) Sei A das Ereignis, dass die erste und die letzte Karte ein Ass sind. Wir fassen A als Teilmenge der Menge aller Kartestapel auf. Damit die erste Karte ein Ass zeigt, haben wir für die erste Position im Stapel 4 Möglichkeiten. Wenn gleichzeitig auch die letzte Karte ein Ass zeigen soll, können wir für diese Position eines der 3 übrigen Asses wählen. Die restlichen 50 Karten werden beliebig auf die restlichen 50 Positionen verteilt. Es ist also $|A| = 4 \cdot 3 \cdot 50!$. Damit folgt

$$p[A] = \frac{12 \cdot 50!}{52!} = \frac{12}{52 \cdot 51} = \frac{1}{221}.$$

- (b) Sei nun B das Ereignis, dass die vier Könige alle hintereinander liegen. Wir betrachten die vier Könige (in irgendeiner festen Reihenfolge) als einen Block. Stellen Sie sich vor, die vier Könige kleben alle aneinander, so dass sie beim Mischen nie getrennt werden. Dann werden beim Mischen 49 Elemente permutiert (der Block an Königen und die 48 übrigen Karten). Es gibt also genau $49!$ Stapel in denen die Könige in unserer fest gewählten Reihenfolge direkt hintereinander liegen. Da es $4!$ Möglichkeiten gibt eine Reihenfolge für die 4 Könige zu wählen, ist $|B| = 49! \cdot 4!$. Damit ist

$$p[B] = \frac{49! \cdot 4!}{52!} = \frac{4!}{52 \cdot 51 \cdot 50} = \frac{1}{5525}.$$

Es ist $A \cap B$ die Menge aller Kartenzustapel in denen an erster und letzter Stelle ein Ass liegt *und* die vier Könige alle hintereinander liegen. Damit ist wie gerade $|A \cap B| = 4 \cdot 3 \cdot 4! \cdot 47!$ und somit

$$p[A \cap B] = \frac{12 \cdot 4! \cdot 47!}{52!} \neq \frac{12 \cdot 50! \cdot 49! \cdot 4!}{52!^2} = p[A] \cdot p[B].$$

Die Ereignisse sind also *nicht* unabhängig (das hätten wir sicher auch intuitiv vermutet, da jede Festlegung von einzelnen Positionen, die Möglichkeiten einschränkt, dass vier gewählte Karten hintereinander liegen).

Lösung von Aufgabe 34 Es sind genau 30 von 90 Steinen rot. Da alle Steine die gleiche Größe haben, gehen wir von einer Gleichverteilung aus. Damit ist die Wahrscheinlichkeit, mit einem Zug einen roten Stein zu ziehen genau $\frac{30}{90} = \frac{1}{3}$.

Nun ziehen wir drei Steine gleichzeitig. Sei B die Menge der blauen Steine, R die Menge der roten Steine und G die Menge der gelben Steine. Wie beim Lottospielen ist der Wahrscheinlichkeitsraum nun gegeben durch die Gleichverteilung p auf $\Omega = \{A \subseteq B \cup R \cup G \mid |A| = 3\}$. Um die Mengen aus Ω zu konstruieren, in denen jede Farbe einmal vorkommt, müssen wir nur einen blauen Stein wählen, einen roten und einen gelben. Dafür haben wir natürlich $20 \cdot 30 \cdot 40$ Möglichkeiten. Die Wahrscheinlichkeit dafür drei Steine unterschiedlicher Farbe zu ziehen ist somit gleich

$$\frac{20 \cdot 30 \cdot 40}{|\Omega|} = \frac{24000}{\binom{90}{3}} = \frac{200}{979} = 0,2042 \dots$$

1.3 Lösungen der Aufgaben aus Kapitel 3

Lösung von Aufgabe 35 In beiden Fällen benutzen wir die Formel aus Beispiel 3.2. Diese liefert:

(a) $a_n = 3^n \cdot 1 + \frac{1-3^n}{1-3} \cdot 2 = 3^n + 3^n - 1 = 2 \cdot 3^n - 1$ für alle $n \in \mathbb{N}_0$.

(b) $a_n = 3^n \cdot (-1) + \frac{1-3^n}{1-3} \cdot 2 = -1$ für alle $n \in \mathbb{N}_0$.

Diese Gleichung findet man auch sobald man $a_1 = -1 = a_0$ berechnet hat. Denn damit ist auch $a_2 = 3 \cdot a_1 + 2 = 3 \cdot a_0 + 2 = a_1$ und so weiter.

Lösung von Aufgabe 36 Wir leiten die Lösung des linearen Gleichungssystems eben her. Falls $\lambda_1 = 0$ ist, ist $\lambda_2 \neq 0$. Weiter ist in diesem Fall

$$\begin{array}{rcl} x_1 + x_2 & = & a_0 \\ \lambda_2 \cdot x_2 & = & a_1 \end{array} \iff \begin{array}{rcl} x_1 + x_2 & = & a_0 \\ x_2 & = & \frac{a_1}{\lambda_2} \end{array} \iff \begin{array}{rcl} x_1 + \frac{a_1}{\lambda_2} & = & a_0 \\ x_2 & = & \frac{a_1}{\lambda_2} \end{array}$$

Damit ist die einzige Lösung des linearen Gleichungssystems gegeben durch $x_1 = a_0 - \frac{a_1}{\lambda_2} = \frac{a_1 - \lambda_2 \cdot a_0}{\lambda_1 - \lambda_2}$ und $x_2 = \frac{a_1}{\lambda_2} = \frac{a_1 - \lambda_1 \cdot a_0}{\lambda_2 - \lambda_1}$.

Sei nun $\lambda_1 \neq 0$. Dann ist

$$\begin{array}{rcl} x_1 & +x_2 & = a_0 \\ \lambda_1 \cdot x_1 + \lambda_2 \cdot x_2 & = a_1 \end{array} \iff \begin{array}{rcl} x_1 + x_2 & = a_0 \\ x_1 + \frac{\lambda_2}{\lambda_1} \cdot x_2 & = \frac{a_1}{\lambda_1} \end{array}$$

Wir ziehen die erste Gleichung von der zweiten ab und erhalten das äquivalente Gleichungssystem

$$\begin{array}{rcl} x_1 + x_2 & = a_0 \\ (\frac{\lambda_2}{\lambda_1} - 1) \cdot x_2 & = \frac{a_1}{\lambda_1} - a_0 \end{array} \iff \begin{array}{rcl} x_1 + x_2 & = a_0 \\ x_2 & = \frac{a_1 - \lambda_1 \cdot a_0}{\lambda_2 - \lambda_1} \end{array}$$

Setzen wir die Lösung für x_2 in die erste Gleichung ein, erhalten wir, dass die einzige Lösung des linearen Gleichungssystems gegeben ist durch $x_1 = a_0 - \frac{a_1 - \lambda_1 \cdot a_0}{\lambda_2 - \lambda_1} = \frac{a_1 - \lambda_2 \cdot a_0}{\lambda_1 - \lambda_2}$ und $x_2 = \frac{a_1 - \lambda_1 \cdot a_0}{\lambda_2 - \lambda_1}$.

Lösung von Aufgabe 37 Mit ein bisschen Tüfteln oder „genauem Hinschauen“ kann man die Aufgabe auch durch ausprobieren lösen. Wir wollen hier jedoch unser Wissen über die geschlossenen Formeln von linearen homogenen Rekursionen der Ordnung 2 benutzen.

Sind $\lambda_1 \neq \lambda_2$ die Nullstellen des charakteristischen Polynoms einer linearen homogenen Rekursion der Ordnung 2, so gilt $a_n = C_1 \cdot \lambda_1^n + C_2 \cdot \lambda_2^n$ für absolute Konstanten C_1 und C_2 . Da diese Konstanten nicht von n abhängen, kann nicht $C_1 \cdot \lambda_1^n + C_2 \cdot \lambda_2^n = 2 \cdot n + 1$ für alle n gelten.

Wir gehen also davon aus, dass das charakteristische Polynom der Rekursion eine doppelte Nullstelle λ besitzt. Dann gilt

$$a_n = C_{10} \cdot \binom{n}{0} \cdot \lambda^n + C_{11} \cdot \binom{n}{1} \cdot \lambda^n = (C_{10} + C_{11} \cdot n) \cdot \lambda^n.$$

Damit dies für alle $n \in \mathbb{N}_0$ gleich $2 \cdot n + 1$ ist, setzen wir $\lambda = 1$ (damit der Faktor λ^n unsichtbar wird) und $C_{10} = 1$ und $C_{11} = 2$. Damit ist das charakteristische Polynom der Rekursion gegeben durch $(x - 1)^2 = x^2 - 2x + 1$, woraus sofort

$$a_n = 2 \cdot a_{n-1} - a_{n-2} \quad \text{für alle } n \geq 2$$

folgt. Die Startwerte sind glücklicherweise schon bekannt: $a_0 = 2 \cdot 0 + 1 = 1$ und $a_1 = 2 \cdot 1 + 1 = 3$.

Lösung von Aufgabe 38 *Induktionsanfang:* $\boxed{k=0}$ Für jedes $m \in \mathbb{N}$ ist $f_0 \cdot f_{m-1} + f_1 \cdot f_m = 1 \cdot f_m = f_{m+0}$. Damit ist der Induktionsanfang gemacht.

Induktionsvoraussetzung: Für beliebiges aber festes $k \in \mathbb{N}_0$ gelte: Für jede natürliche Zahl $m \in \mathbb{N}$ ist $f_{k+m} = f_k \cdot f_{m-1} + f_{k+1} \cdot f_m$.

Induktionsschritt: $\boxed{k \rightarrow k+1}$ Wir zeigen, dass die Behauptung auch für $k+1$ gilt. Sei also $m \in \mathbb{N}$ beliebig, dann ist

$$\begin{aligned}
& f_{k+1} \cdot f_{m-1} + f_{k+2} \cdot f_m \\
&= f_{k+1} \cdot f_{m-1} + (f_{k+1} + f_k) \cdot f_m \\
&= f_{k+1} \cdot (f_{m-1} + f_m) + f_k \cdot f_m \\
&= f_k \cdot f_m + f_{k+1} \cdot f_{m+1}
\end{aligned} \tag{1.5}$$

Hier haben wir nur zweimal die Definition der Fibonacci-Zahlen benutzt. Da unsere Induktionsvoraussetzung für jedes $m \in \mathbb{N}$ gilt (die Bedingung hängt nur von k ab), gilt Sie auch für $m + 1$. Damit ist (1.5) gleich $f_{k+(m+1)} = f_{(k+1)+m}$ und die Aussage ist bewiesen.

Lösung von Aufgabe 39 Da die Rekursionsvorschrift für die Lucas-Zahlen L_n genau die gleiche ist, wie die der Fibonacci-Zahlen (die Rekursion unterscheidet sich nur durch die veränderten Startwerte), kennen wir das charakteristische Polynom bereits – es ist

$$x^2 - x - 1 = \left(x - \frac{1 + \sqrt{5}}{2}\right) \cdot \left(x - \frac{1 - \sqrt{5}}{2}\right).$$

Damit gilt für alle $n \in \mathbb{N}_0$ die Gleichung $L_n = C_1 \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n + C_2 \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n$ für gewisse Konstanten C_1 und C_2 . Für $n = 0$ und $n = 1$ erhalten wir das Gleichungssystem

$$\begin{aligned}
1 \cdot C_1 + 1 \cdot C_2 &= 2 \\
\frac{1 + \sqrt{5}}{2} \cdot C_1 + \frac{1 - \sqrt{5}}{2} \cdot C_2 &= 1
\end{aligned}$$

Das können wir schnell lösen oder die Formel aus Aufgabe 36 benutzen. Wir erhalten $C_1 = C_2 = 1$ und somit die geschlossene Formel

$$L_n = \left(\frac{1 + \sqrt{5}}{2}\right)^n + \left(\frac{1 - \sqrt{5}}{2}\right)^n \quad \text{für alle } n \in \mathbb{N}_0$$

Lösung von Aufgabe 40 Da die geschlossene Formel der Rekursion nur aus zwei Summanden besteht, gehen wir davon aus, dass es sich um eine lineare homogene Rekursion der Ordnung 2 handelt. Das charakteristische Polynom dieser Rekursion muss dann genau die beiden Nullstellen $1 + \sqrt{3}$ und $1 - \sqrt{3}$ haben. Damit ist das charakteristische Polynom gleich

$$(x - (1 + \sqrt{3})) \cdot (x - (1 - \sqrt{3})) = x^2 - 2 \cdot x - 2$$

und die Rekursion gegeben durch

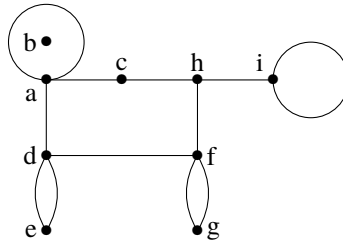
$$a_n = 2 \cdot a_{n-1} + 2 \cdot a_{n-2} \quad \text{für alle } n \geq 2.$$

Wir müssen also nur noch die Startwerte $a_0 = (1 + \sqrt{3})^0 + (1 - \sqrt{3})^0 = 2$ und $a_1 = (1 + \sqrt{3})^1 + (1 - \sqrt{3})^1 = 2$ berechnen.

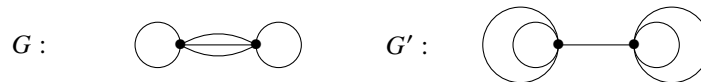
Lösung von Aufgabe 41 Wir stellen zunächst fest, dass die Teile gleicher Farbe auch gleichgroß sind. Damit erhalten wir immer den gleichen Flächeninhalt, egal wie wir die vier Teile zusammensetzen. Damit können die beiden großen „Dreiecke“ nicht deckungsgleich sein. Es folgt, dass die Zusammensetzungen der vier Teile keine(!) Dreiecke liefert. Im linken Bild ist die „Hypothense“ leicht nach außen gedrückt und im rechten Bild leicht nach innen (wenn man das einmal weiß, dann sieht man es auch mit bloßem Auge). Dass dieser Knick so schwer zu sehen ist liegt daran, dass sich die Steigung des roten Dreiecks ($\frac{2}{5} = \frac{f_3}{f_5}$) kaum von der des grünen Dreiecks ($\frac{3}{8} = \frac{f_4}{f_6}$) unterscheidet. Hier bezeichnet f_n die n -te Fibonacci-Zahl. Mit Bemerkung 3.13 sind beide Quotienten gute Annäherungen an $(\frac{2}{1+\sqrt{5}})^2$.

1.4 Lösungen der Aufgaben aus Kapitel 4

Lösung von Aufgabe 42 Eine von unzähligen Möglichkeiten ist die folgende:

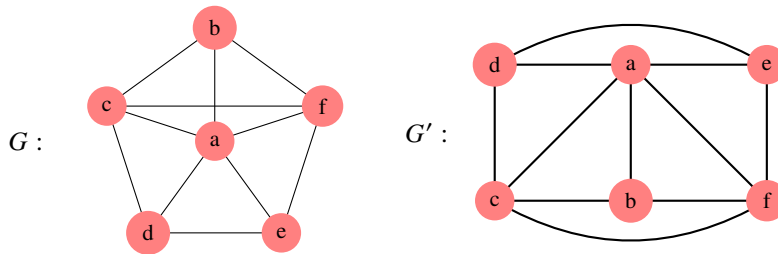


Lösung von Aufgabe 43 Dies kann nur für Graphen funktionieren, die nicht einfach sind. Ein Beispiel sind die Graphen



Jede Ecke von G ist sowohl mit sich selbst als auch mit der anderen Ecke benachbart. Das gleiche gilt für die Ecken von G' . Weiter haben alle Ecken den Grad 5. Trotzdem sind G und G' offensichtlich nicht isomorph, da G zwei Schleifen besitzt und G' vier Schleifen.

Lösung von Aufgabe 44 Die beiden Graphen G und G' sind isomorph, wie die folgende Beschriftung zeigt. Da die Graphen einfach sind, genügt es die Ecken passend zu beschriften.



Auf diese Beschriftung stösst man, wenn man zunächst den Graphen G irgendwie beschriftet. Dann muss die einzige Ecke in G' vom Grad 5 genauso beschriftet werden wie die einzige Ecke von Grad 5 in G (in unserem Fall mit a). Den beiden Ecken vom Grad 4 in G' ordnen Sie irgendwie die beiden Ecken vom Grad 4 aus G' zu (in unserem Fall c und f). Die Beschriftung der übrigen Ecken ergibt sich dann sofort aus den Nachbarschaftsrelationen.

Lösung von Aufgabe 45 Sei k eine Kante von G , die die Ecken e und f verbindet.

Zu (a): Wenn diese Aussage für Sie anschaulich klar ist, brauchen Sie die folgende Lösung nicht zu lesen.

Ist k in einem echten Kreis enthalten, dann gibt es einen Weg von e nach f , der k nicht benutzt (entfernen wir aus einem Kreis genau eine Kante, bleibt immer noch ein Weg übrig). Sind nun a und b beliebige Ecken aus einer Zusammenhangskomponente von G . Wir wählen irgendeinen Weg von a nach b . Falls dieser Weg die Kante k benutzt, können wir k auch durch den Weg zwischen e und f ersetzen, der k nicht benutzt. Das heißt: zwischen a und b gibt es immer einen Weg, der k nicht benutzt. Insbesondere gibt es auch einen Weg von a nach b in $G \setminus \{k\}$, was nichts anderes bedeutet, als dass a und b in der selben Zusammenhangskomponente von $G \setminus \{k\}$ sind. Damit besitzt G genauso viele Zusammenhangskomponenten wie $G \setminus \{k\}$ und k ist keine Brücke. Betrachten wir die Kontraposition der gezeigten Implikation erhalten wir

$$k \text{ ist eine Brücke} \iff k \text{ ist in keinem echten Kreis enthalten}$$

Sei nun k nicht in einem echten Kreis enthalten. Dann gibt es keinen Weg von e nach f , der k nicht benutzt. Insbesondere gibt es keinen Weg von e nach f in $G \setminus \{k\}$ und e und f sind in verschiedenen Zusammenhangskomponenten von $G \setminus \{k\}$. Also besitzt $G \setminus \{k\}$ mehr Zusammenhangskomponenten als G und k ist eine Brücke. Damit ist auch die Rückrichtung gezeigt.

Zu (b): Zeichnen wir eine weitere Kante in einen Graphen, so verbinden wir höchstens zwei Ecken mit einander (genau zwei, wenn wir keine Schleife zeichnen). Damit können wir höchstens zwei Zusammenhangskomponenten verbinden. Insbesondere hat G höchstens eine Zusammenhangskomponente weniger als $G \setminus \{k\}$. Wir formulieren den Satz um und erhalten, dass $G \setminus \{k\}$ höchstens eine Zusammenhangskomponente mehr hat als G .

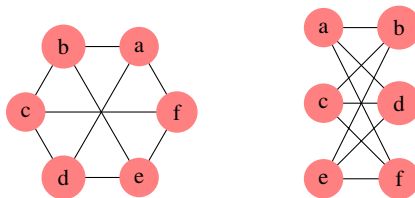
Lösung von Aufgabe 46 Zu (a): Nach Definition hat H_5 genau $|\{0, 1\}^5| = 2^5$ Ecken. Weiter sind zwei Ecken $(a_1, \dots, a_5), (b_1, \dots, b_5) \in E(H_5) = \{0, 1\}^5$ genau dann benachbart, wenn sie sich in genau einem Eintrag unterscheiden. Damit ist jede Ecke mit genau fünf anderen benachbart, was bedeutet, dass jede Ecke Grad 5 hat. Es folgt

$$2 \cdot |K(H_5)| = \sum_{(a_1, \dots, a_5) \in E(H_5)} d((a_1, \dots, a_5)) = \sum_{(a_1, \dots, a_5) \in E(H_5)} 5 = 2^5 \cdot 5$$

und somit besitzt H_5 genau $2^4 \cdot 5 = 2^3 \cdot 10 = 80$ Kanten.

Zu (b): Wir benutzen, dass ein Graph genau dann bipartit ist, wenn es keine Kreise ungerader Länge in diesem Graphen gibt. Sei also $e_0, k_1, e_1, k_2, e_2, \dots, k_r, e_r$ mit $e_r = e_0 = (a_1, \dots, a_n) \in \{0, 1\}^n$ irgendein Kreis in H_n . Für alle $i \in \{1, \dots, r\}$ unterscheiden sich e_i und e_{i-1} in genau einem Eintrag (beachte, dass unsere Ecken Elemente aus $\{0, 1\}^n$ sind). Da $e_0 = e_r$ ist, wurde jeder Eintrag in einer geraden Anzahl von Schritten verändert. Damit muss der Kreis aus einer geraden Anzahl von Schritten bestehen, was nichts anderes bedeutet, als dass die Länge des Kreises (r) eine gerade Zahl ist. Da der Kreis beliebig gewählt war, gibt es keine Kreise ungerader Länge in H_n und H_n ist damit bipartit.

Lösung von Aufgabe 47 Dass die beiden Graphen isomorph sind, sieht man an der folgenden Beschriftung.



Lösung von Aufgabe 48 Der Graph G besitzt genau eine Ecke mehr als Kanten. Damit ist G ein Baum. Ein Baum ist ein zusammenhängender Graph ohne echte Kreise. Insbesondere gibt es in G keine Kreise von gerader Länge. Damit ist G bipartit.

Lösung von Aufgabe 49 Sei G irgendein zusammenhängender Graph. Wir konstruieren einen Graphen G' aus G in dem wir jede Kante doppelt einzeichnen. Dadurch sind an jeder Ecke von G' genau doppelt so viele Kanten eingezeichnet, wie an der entsprechenden Ecke von G . Insbesondere ist der Grad jeder Ecke aus G' gerade und somit ist G' eulersch. Es gibt also einen Kreis in G' , der jede Kante von G' genau einmal benutzt. Fassen wir nun die verdoppelten Kanten wieder zu einer zusammen erhalten wir, dass es einen Kreis in G gibt, der jede Kante aus G genau zweimal benutzt.

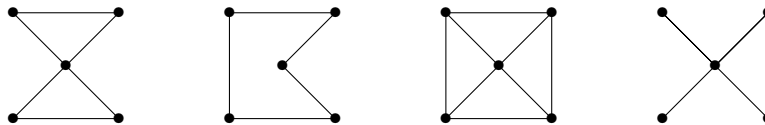
Lösung von Aufgabe 50 Wir zeichnen die Personen als Punkte und verbinden je zwei Punkte mit einander. Damit erhalten wir den vollständigen Graphen K_n auf n

Ecken. Geben sich nun zwei Personen die Hand, zeichnen wir die Kante zwischen diesen Personen beiden nach. Da sich alle Personen untereinander genau einmal die Hand geben sollen, wollen wir also jede Kante des K_n genau einmal nachzeichnen. Nun soll immer eine Person zweimal hintereinander die Hand reichen. Im Bild bedeutet dies nichts anderes, als dass zwei Kanten, die wir nacheinander zeichnen auch einen gemeinsamen Endpunkt brauchen.

Fassen wir alles zusammen erhalten wir, dass sich n Personen genau dann auf die beschriebene Art die Hände reichen können, wenn es einen eulerschen Weg im K_n gibt. Dies ist genau dann der Fall, wenn maximal zwei Ecken des K_n ungeraden Grad besitzen. Allerdings ist der Grad jeder Ecke gleich $n-1$ und es ist nach Voraussetzung $n \geq 3$. Damit gibt es im K_n genau dann einen eulerschen Weg, wenn $n-1$ gerade ist – sprich: wenn n ungerade ist.

Lösung von Aufgabe 51 Wir fassen das Bild als Graph auf in dem wir jeden Schnittpunkt als Ecke realisieren. Als Schnittpunkt von zwei Kreisen, hat jede Ecke den Grad 4. Insbesondere ist der Grad jeder Ecke gerade und der Graph ist eulersch. Damit lässt sich der Graph (und somit das Bild) zeichnen ohne den Stift abzusetzen und ohne eine Kante mehrfach zu zeichnen.

Lösung von Aufgabe 52 Wir betrachten die vier Graphen



Der erste Graph ist offensichtlich eulersch. Hamiltonsch ist er jedoch nicht: Es gibt nur einen Kreis, der jede Ecke benutzt, und der benutzt die Ecke in der Mitte zweimal.

Im zweiten Graph gibt es nur einen echten Kreis. Dieser ist offensichtlich sowohl eulersch als auch hamiltonsch.

Der dritte Graph ist nicht eulersch, da es vier Ecken von ungeradem Grad gibt. Der Graph ist hamiltonsch, da er den zweiten Graph als Teilgraph besitzt.

Im vierten Graphen gibt es keine echten Kreise. Insbesondere ist er also weder eulersch noch hamiltonsch.

Lösung von Aufgabe 53 Wir beweisen den Satz mit den vorgegebenen Schritten.

Zu (a): Da H einfach ist, gibt der Grad einer Ecke genau die Anzahl von Nachbarn dieser Ecke an. Sind nun e und f zwei Ecken, die nicht benachbart sind. Sei A_e die Teilmenge von $E(H)$, die aus genau den Nachbarn von e besteht, und sei A_f die Teilmenge, die aus den Nachbarn von f besteht. Es ist $A_e \subseteq E(H) \setminus \{e, f\}$ und $A_f \subseteq E(H) \setminus \{e, f\}$. Insbesondere ist also $A_e \cup A_f \subseteq E(H) \setminus \{e, f\}$. Weiter ist nach Voraussetzung $|A_e| = d(e) \geq \frac{n}{2}$ und $|A_f| = d(f) \geq \frac{n}{2}$. Nun können A_e und A_f nicht disjunkt sein, da sonst $|A_e \cup A_f| \geq \frac{n}{2} + \frac{n}{2} = n$ wäre, im Widerspruch zu $|E(H)| = n-2$. Dass A_e und A_f nicht disjunkt sind bedeutet nichts anderes als dass es einen gemeinsamen Nachbarn von e und f gibt.

Zu (b): Das sieht schlimmer aus als es ist. Als erstes stellen wir fest, dass das G aus der Aufgabenstellung nicht der K_n ist, da dieser offensichtlich hamiltonsch ist. Nach Annahme gilt für G folgendes: Wenn wir eine weitere Kante in G einzeichnen, so ist G hamiltonsch.

Wir zeichnen also irgendeine (neue) Kante in den Graphen G und erhalten einen hamiltonschen Kreis

$$e_1 k_1 e_2 k_2 \dots k_n e_n k_{n+1} \underbrace{e_{n+1}}_{=e_1}.$$

Irgendeine der Kanten, muss die neu eingezeichnete Kante sein, da sonst G hamiltonsch wäre. In einem Kreis können wir jede Ecke als Startpunkt wählen. Daher können wir ohne weiteres annehmen, dass k_{n+1} die neue Kante ist. Da der Kreis hamiltonsch ist, kommt k_{n+1} nicht nochmal in diesem Weg vor. Damit ist

$$e_1 k_1 e_2 k_2 \dots k_n e_n \quad (1.6)$$

ein hamiltonscher Weg in G .

Zu (c): Da der Weg aus (1.6) hamiltonsch ist, ist $E(G) = \{e_1, \dots, e_n\}$ und $|E(G)| = n$. Wir setzen nun

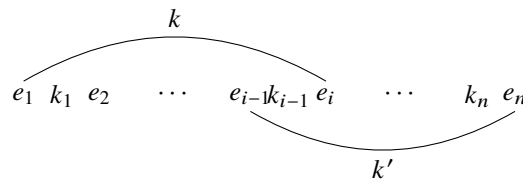
$$\begin{aligned} A_1 &= \{e_j \in E(G) | e_j \text{ und } e_1 \text{ sind benachbart}\} \\ A_n &= \{e_j \in E(G) \setminus \{e_1\} | e_{j-1} \text{ und } e_n \text{ sind benachbart}\} \end{aligned}$$

(beachten Sie, den Index in der zweiten Menge!). Wie in (a) ist $A_1 \cup A_n \subseteq E(G) \setminus \{e_1\}$ und somit

$$|A_1 \cup A_n| \leq n - 1. \quad (1.7)$$

Allerdings ist wieder $|A_1| = d(e_1) \geq \frac{n}{2}$ und $|A_n| = d(e_n) \geq \frac{n}{2}$. Damit ist mit (1.7) $|A_1 \cup A_n| \neq |A_1| + |A_n| = n$, was sofort impliziert, dass es ein Element e_i im Schnitt von A_1 und A_n gibt. Das war zu zeigen.

Zu (d): Wir benutzen die Notation aus Teil (c). Dann gibt es eine Kante k zwischen e_1 und e_i und eine Kante k' zwischen e_{i-1} und e_n . Wir haben also



Jetzt kann man den hamiltonschen Kreis einfach ablesen: Wir laufen wie gehabt von e_1 nach e_{i-1} , gehen von da aus über k' nach e_n , laufen den Weg dann rückwärts zu e_i und laufen von da aus über k zurück zu e_1 . D. h.:

$$e_1 k_1 e_2 \cdots k_{i-2} e_{i-1} k' e_n k_n e_{n-1} k_{n-1} e_{n-2} \cdots k_{i+1} e_i k e_1$$

Dieser Kreis ist offensichtlich hamiltonisch.

Zu (e): Eigentlich ist der Beweis nun schon beendet. Angenommen es gibt einen einfachen zusammenhängenden Graphen auf $n \geq 3$ Ecken, der nicht hamiltonisch ist und in dem jede Ecke mindestens Grad $\frac{n}{2}$ besitzt. Dann gibt es (mindestens) einen solchen Graphen, der maximal ist bezüglich der Anzahl von Kanten. Sei G solch ein Graph (das ist der Graph aus (b)). In (d) haben wir gezeigt, dass es einen hamiltonischen Kreis in G gibt, im Widerspruch zur Annahme, dass G nicht hamiltonisch ist. Damit muss die Annahme falsch gewesen sein. Es gibt also keinen einfachen zusammenhängenden Graphen auf $n \geq 3$ Ecken in dem jede Ecke mindestens Grad $\frac{n}{2}$ besitzt.

Lösung von Aufgabe 54 Eine 2-Kantenfärbung von K_n mit den Farben aus T ist eine Abbildung $\Psi : K(K_n) \rightarrow T$. Da $|K(K_n)| = \binom{n}{2}$ und $|T| = 2$, gibt es genau $2^{\binom{n}{2}}$ verschiedene solcher Abbildungen.

(Sie haben für jede der $\binom{n}{2}$ Kanten von K_n eine Wahl zwischen 2 Farben.)

Lösung von Aufgabe 55 Wir wollen zeigen, dass $R(r, b) \leq \binom{r+b-2}{r-1}$ für alle $r, b \in \mathbb{N}$ gilt. Aus dem Beweis von Theorem 4.41 wissen wir, dass

- (i) $R(r, 1) = R(1, b) = 1$ und
- (ii) $R(r, b) \leq R(r-1, b) + R(r, b-1)$ für $r, b \leq 2$.

Mit den üblichen Rechenregeln für den Binomialkoeffizienten, wissen wir auch

- (1) $\binom{1+b-2}{1-1} = \binom{r+1-2}{r-1} = 1$ und
- (2) $\binom{r+b-2}{r-1} = \binom{(r-1)+b-2}{(r-1)-1} + \binom{r+(b-1)-2}{r-1}$ für $r, b \leq 2$.

Damit ist die Behauptung fast offensichtlich. Um das *fast* aus diesem Satz zu radieren führen wir eine Induktion über $r + b$.

Im *Induktionsanfang* ist $r + b = 2$ und somit $r = b = 1$. Die Aussagen aus (i) und (1) liefern also $R(r, b) = \binom{r+b-2}{r-1}$ und somit insbesondere $R(r, b) \leq \binom{r+b-2}{r-1}$.

Als *Induktionsvoraussetzung* nehmen wir an, dass für beliebiges aber festes $n \in \mathbb{N}$ für alle $r, b \in \mathbb{N}$, mit $r + b = n$, die Ungleichung $R(r, b) \leq \binom{r+b-2}{r-1}$ gilt.

Für den *Induktionsschritt* sei nun $r + b = n + 1$. Falls $r = 1$ oder $b = 1$, folgt die Behauptung aus den Aussagen in (i) und (1). Falls r und b größer als 1 sind, gilt

$$R(r, b) \stackrel{(ii)}{\leq} R(r-1, b) + R(r, b-1) \stackrel{IV}{\leq} \binom{(r-1)+b-2}{(r-1)-1} + \binom{r+(b-1)-2}{r-1} \stackrel{(2)}{=} \binom{r+b-2}{r-1}$$

(beachte, dass tatsächlich $(r-1) + b = r + (b-1) = n$ ist). Das war zu zeigen.

Lösung von Aufgabe 56 Der Graoh $K_{3,3}$ besitzt als bipartiter Graph keine echten Kreise ungerader Länge. Weiter ist $K_{3,3}$ einfach und besitzt daher keine echten Kreise der Länge 2. Damit hat jeder echte Kreis in $K_{3,3}$ mindestens die Länge 4.

Angenommen $K_{3,3}$ wäre planar, dann wäre mit unserer Vorüberlegung jede Fläche durch mindestens 4 Kanten begrenzt. Da jede Kante maximal zwei Flächen trennt,

wäre die Anzahl von Flächen somit höchstens gleich $2 \cdot \frac{|K(K_{3,3})|}{4} = \frac{9}{2}$. Die Eulersche-Formel besagt aber, dass die Anzahl von Flächen genau $|K(K_{3,3})| + 2 - |E(K_{3,3})| = 9 + 2 - 6 = 5 > \frac{9}{2}$ ist. Das ist ein Widerspruch und somit ist $K_{3,3}$ nicht planar.

1.5 Lösungen der Aufgaben aus Kapitel 5

Lösung von Aufgabe 57 Da für alle $a \in \mathbb{Z}$ gilt $a \mid a$, ist \sim reflexiv. Weiter ist für $a, b \in \mathbb{Z}$

$$a \sim b \iff a \mid b \text{ oder } b \mid a \iff b \sim a.$$

Damit ist \sim auch symmetrisch. Allerdings ist \sim nicht transitiv. Denn: Es ist $2 \sim 10$ und $10 \sim 5$, aber es gilt nicht $2 \sim 5$, da weder $2 \mid 5$ noch $5 \mid 2$ gilt. Insbesondere ist \sim keine Äquivalenzrelation.

Lösung von Aufgabe 58 Wir übersetzen die Gleichung zunächst in eine Relation zwischen Äquivalenzklassen. Dazu schreiben wir a als $[(a_1, a_2)]$, b als $[(b_1, b_2)]$ und c als $[(c_1, c_2)]$, mit $a_1, a_2, b_1, b_2, c_1, c_2 \in \mathbb{N}_0$. Dann müssen wir zeigen, dass

$$[(a_1, a_2)] \odot ([[(b_1, b_2)] \oplus [(c_1, c_2)]] \sim [(a_1, a_2)] \odot [(b_1, b_2)] \oplus [(a_1, a_2)] \odot [(c_1, c_2)] \quad (1.8)$$

gilt. Nur mit Benutzung der Definition der Addition \oplus und der Multiplikation \odot ist (1.8) äquivalent zu

$$[(a_1, a_2)] \odot ([[(b_1 + c_1, b_2 + c_2)]] \sim [(a_1 \cdot b_1 + a_2 \cdot b_2, a_1 \cdot b_2 + a_2 \cdot b_1)] \oplus [(a_1 \cdot c_1 + a_2 \cdot c_2, a_1 \cdot c_2 + a_2 \cdot c_1)],$$

was wiederum äquivalent ist zu

$$[(a_1 \cdot (b_1 + c_1) + a_2 \cdot (b_2 + c_2), a_1 \cdot (b_2 + c_2) + a_2 \cdot (b_1 + c_1))] \sim [(a_1 \cdot b_1 + a_2 \cdot b_2 + a_1 \cdot c_1 + a_2 \cdot c_2, a_1 \cdot b_2 + a_2 \cdot b_1 + a_1 \cdot c_2 + a_2 \cdot c_1)].$$

Die Rechnungen innerhalb der Klammern sind alles Rechnungen in \mathbb{N}_0 . Wir dürfen also das Distributivgesetz auf \mathbb{N}_0 benutzen. Damit sehen wir, dass die letzte Relation erfüllt ist. Damit gilt auch (1.8) und somit das Distributivgesetz auf \mathbb{Z} .

Lösung von Aufgabe 59 Im folgenden seien stets $a, b, c \in \mathbb{Z}$.

Zu (a): Es ist $1 \cdot a = a = a \cdot 1$. Da 1 und a ganze Zahlen sind, folgt mit der Definition der Teilbarkeit, dass $1 \mid a$ und $a \mid a$ gilt.

Zu (b): Es ist $a \mid b$

$$\begin{aligned} \iff \exists k \in \mathbb{Z}, \text{ mit } a \cdot k = b &\iff \exists k \in \mathbb{Z}, \text{ mit } (-1) \cdot a \cdot \underbrace{(-1) \cdot k}_{\in \mathbb{Z}} = b \\ \iff \exists k' \in \mathbb{Z}, \text{ mit } (-1) \cdot a \cdot k' = b &\iff (-1) \cdot a \mid b \end{aligned}$$

Zu (c): Sei nun $c \neq 0$. Wir beweisen die beiden Implikationen vorsichtshalber nacheinander.

\Rightarrow Dass a ein Teiler von b ist, bedeutet genau, dass es ein $k \in \mathbb{Z}$ gibt mit $a \cdot k = b$. Damit ist aber natürlich auch $(a \cdot c) \cdot k = (a \cdot k) \cdot c = b \cdot c$. Per Definition der Teilbarkeit bedeutet dies $a \cdot c \mid b \cdot c$ (Bis jetzt haben wir $c \neq 0$ noch nicht gebraucht).

\Leftarrow Ist nun $a \cdot c \mid b \cdot c$, so gibt es ein $k \in \mathbb{Z}$ mit $(a \cdot c) \cdot k = b \cdot c$. Damit folgt

$$0 = (a \cdot c) \cdot k - b \cdot c = (a \cdot k - b) \cdot c.$$

Nach Voraussetzung ist $c \neq 0$ und wir wissen bereits, dass \mathbb{Z} nullteilerfrei ist. Damit muss $0 = a \cdot k - b$ – also $a \cdot k = b$ – gelten, was nichts anderes heißt als $a \mid b$.

Zu (d): Es gilt: $a \mid b \implies \exists k \in \mathbb{Z}, \text{ mit } a \cdot k = b \implies \exists k \in \mathbb{Z}, \text{ mit } a \cdot (c \cdot k) = c \cdot (a \cdot k) = c \cdot b \implies \exists k' \in \mathbb{Z}, \text{ mit } a \cdot k' = c \cdot b \implies a \mid c \cdot b$.

Zu (e): Wurde bereits bewiesen.

Zu (f): Aus $a \mid b$ und $b \mid c$ folgt, dass es $k, k' \in \mathbb{Z}$ gibt, mit $a \cdot k = b$ und $b \cdot k' = c$. Setzen wir nun die erste Gleichung in die zweite ein, so erhalten wir $(a \cdot k) \cdot k' = c$ – und somit $a \cdot (k \cdot k') = c$. Da $k \cdot k'$ eine ganze Zahl ist, folgt sofort $a \mid c$.

Lösung von Aufgabe 60 Angenommen, es gäbe $x, y, z \in \mathbb{Z}$, die die Gleichung erfüllen. Dann ist

$$8 = 18 \cdot x^2 - 6 \cdot y + 42 \cdot z^3 = 3 \cdot \underbrace{(6 \cdot -2 \cdot y + 14 \cdot z^3)}_{\in \mathbb{Z}},$$

und somit gilt $3 \mid 8$. Das ist natürlich Nonsense und somit muss die Annahme falsch gewesen sein: Es gibt somit keine Lösung der Gleichung in den ganzen Zahlen.

Lösung von Aufgabe 61 Wir berechnen zunächst die Summe ohne eine Einschränkung an $n \in \mathbb{N}$. Es ist

$$\sum_{i=0}^{n-1} (k+i) = \sum_{i=0}^{n-1} k + \sum_{i=0}^{n-1} i = n \cdot k + \frac{n \cdot (n-1)}{2}.$$

Hier haben wir die bekannte Summenformel für die ersten $n-1$ natürlichen Zahlen benutzt. Ist nun n ungerade, so ist $n-1$ gerade und damit $\frac{n-1}{2} \in \mathbb{Z}$. Es folgt

$$\sum_{i=0}^{n-1} (k+i) = n \cdot k + \frac{n \cdot (n-1)}{2} = n \cdot \underbrace{\left(k + \frac{n-1}{2}\right)}_{\in \mathbb{Z}}$$

und somit $n \mid \sum_{i=0}^{n-1} (k+i)$.

Falls nun n gerade ist, so ist immer noch $\sum_{i=0}^{n-1} (k+i) = n \cdot \left(k + \frac{n-1}{2}\right)$. Aber nun ist $2 \nmid n-1$ und somit ist der Faktor in der Klammer keine ganze Zahl. Damit gibt es keine ganze Zahl k' mit $n \cdot k' = \sum_{i=0}^{n-1} (k+i)$. Für ein gerades n ist somit $n \nmid \sum_{i=0}^{n-1} (k+i)$.

Lösung von Aufgabe 62 Wir berechnen $f(1) = f(2) = f(3) = f(4) = 0$. Dann ist (nach dem Fundamentalsatz der Algebra) $f(x) = (x-1) \cdot (x-2) \cdot (x-3) \cdot (x-4)$. Sei nun $n \in \mathbb{Z}$ beliebig. Dann ist $f(n)$ das Produkt von vier aufeinanderfolgenden ganzen Zahlen. Genau zwei dieser Faktoren sind gerade und genau einer der Faktoren ist durch 4 teilbar. Damit ist das Produkt $f(n)$ durch $2 \cdot 4 = 8$ teilbar. (Es ist zusätzlich noch mindestens einer der Faktoren durch 3 teilbar, woraus wir sogar $24 \mid f(n)$ schließen können).

Sie können auch ganz direkt $n = 4 \cdot q + r$, mit $r \in \{0, 1, 2, 3\}$ schreiben und $q \in \mathbb{Z}$, was wir Dank Division mit Rest tun dürfen. Dann ist

$$f(n) = (n-1) \cdot (n-2) \cdot (n-3) \cdot (n-4) = (4 \cdot q + r - 1) \cdot (4 \cdot q + r - 2) \cdot (4 \cdot q + r - 3) \cdot (4 \cdot q + r - 4).$$

Da $r \in \{0, 1, 2, 3\}$, sieht man direkt, dass einer der Faktoren durch 4 teilbar ist und ein weiterer durch 2. Damit ist $2 \cdot 4 \mid f(n)$.

Lösung von Aufgabe 63 Zu (a): Sei $c \in \mathbb{Z}$ ein gemeinsamer Teiler von a und b . Dann ist $c \mid a$ und $c \mid b$, und somit auch $c \mid a + b$. Insbesondere ist c auch ein gemeinsamer Teiler von a und $a + b$.

Ist nun $c \in \mathbb{Z}$ ein gemeinsamer Teiler von a und $a + b$, dann folgt genau wie gerade $c \mid (a + b) - a = b$. Damit ist c auch ein gemeinsamer Teiler von a und b .

Wir haben gezeigt, dass die Menge der gemeinsamen Teiler von a und b gleich der Menge der gemeinsamen Teiler von a und $a + b$ ist. Damit ist insbesondere der größte gemeinsame Teiler von a und b gleich dem größten gemeinsamen Teiler von a und $a + b$.

Zu (b): Wir geben eine ausführliche Rechnung nur im ersten Fall an. Für die restlichen Fälle präsentieren wir nur Ergebnisse. Dabei ist es wichtig zu beachten, dass die Ergebnisse für x und y nicht eindeutig sind – eine andere Wahl von x und y als die hier angegebene, kann die Gleichung genauso gut erfüllen.

- Wir starten natürlich mit dem Euklidischen Algorithmus:

$$225 = 1 \cdot 162 + 63$$

$$162 = 2 \cdot 63 + 36$$

$$63 = 1 \cdot 36 + 27$$

$$36 = 1 \cdot 27 + 9$$

$$27 = 3 \cdot 9 + 0$$

$\Rightarrow \text{ggT}(225, 162) = 9$. Rückwärtsrechnen liefert

$$\begin{aligned}
 9 &= 36 - 27 = 36 - (63 - 36) = 2 \cdot 36 - 63 = 2 \cdot (162 - 2 \cdot 63) - 63 \\
 &= 2 \cdot 162 - 5 \cdot 63 = 2 \cdot 162 - 5 \cdot (225 - 162) \\
 &= 7 \cdot 162 - 5 \cdot 225
 \end{aligned}$$

Damit ist $x = -5$ und $y = 7$.

- $\text{ggT}(144, 100) = 4$, $x = -9$ und $y = 13$
- $\text{ggT}(332211, 112233) = 33$, $x = 25$ und $y = -74$
- $\text{ggT}(1909, 1660) = 83$, $x = 7$ und $y = -8$

Lösung von Aufgabe 64 Das Lemma von Bézout sagt uns, dass es mindestens ein solches Tupel $(x, y) \in \mathbb{Z}^2$ gibt. Aus diesem können wir nun aber ganz leicht beliebig viele weitere konstruieren. Sei dazu $k \in \mathbb{Z}$ beliebig. Dann ist

$$d = a \cdot x + b \cdot y + (a \cdot b \cdot k - a \cdot b \cdot k) = a \cdot (x + b \cdot k) + b \cdot (y - a \cdot k).$$

Damit ist also auch $(x + b \cdot k, y - a \cdot k) \in \mathbb{Z}^2$ ein Tupel, das die Gleichung löst. Da $a \neq 0$ ist, liefert jedes $k \in \mathbb{Z}$ ein anderes Tupel – also gibt es unendlich viele.

Lösung von Aufgabe 65 Sei f_n die n -te Fibonacci-Zahl. Wir wissen bereits, dass $\text{ggT}(f_n, f_{n+1}) = 1$ ist für alle $n \in \mathbb{N}$. Damit gibt es $x, y \in \mathbb{Z}$ mit $f_n \cdot x + f_{n+1} \cdot y = 1$. Wir berechnen x und y für die ersten paar $n \geq 3$:

$$1 = (-1) \cdot f_3 + 1 \cdot f_4$$

$$1 = 2 \cdot f_4 + (-1) \cdot f_5$$

$$1 = (-3) \cdot f_5 + 2 \cdot f_6$$

$$1 = 5 \cdot f_6 + (-3) \cdot f_7$$

Schauen wir uns die Faktoren des ersten Summanden an $((-1), 2, (-3), 5)$ sehen, wir dass diese gleich $-f_2, f_3, -f_4, f_5$ sind. Die Faktoren des zweiten Summanden sind $f_1, -f_2, f_3, -f_4$. Wir vermuten also, dass diese Folgen genauso weiter gehen.

Vermutung: Für alle natürlichen Zahlen $n \geq 3$ gilt

$$f_n \cdot (-1)^n \cdot f_{n-1} + f_{n+1} \cdot (-1)^{n+1} \cdot f_{n-2} = 1 \quad (1.9)$$

Dies wollen wir per Induktion über n beweisen, wobei wir den *Induktionsanfang* ($n = 3$) bereits erledigt haben. Als *Induktionsvoraussetzung* nehmen wir nun an, dass für beliebiges aber festes $n \geq 3$ die Gleichung (1.9) gilt. Im *Induktionsschritt* zeigen wir nun, dass damit (1.9) auch für $n + 1$ gilt. Wir berechnen also

$$\begin{aligned}
& f_{n+1} \cdot (-1)^{n+1} \cdot f_n + f_{n+2} \cdot (-1)^{n+2} \cdot f_{n-1} \\
&= f_{n+1} \cdot (-1)^{n+1} \cdot f_n + (f_{n+1} + f_n) \cdot (-1)^n \cdot f_{n-1} \\
&= f_{n+1} \cdot \left((-1)^{n+1} \cdot f_n + (-1)^n \cdot f_{n-1} \right) + f_n \cdot (-1)^n \cdot f_{n-1} \\
&= f_{n+1} \cdot (-1)^{n+1} \cdot (f_n - f_{n-1}) + f_n \cdot (-1)^n \cdot f_{n-1} \\
&= f_{n+1} \cdot (-1)^{n+1} \cdot f_{n-2} + f_n \cdot (-1)^n \cdot f_{n-1} \stackrel{IV}{=} 1
\end{aligned}$$

Damit ist die Vermutung bewiesen und die Aufgabe gelöst.

Lösung von Aufgabe 66 Wir zeigen, dass sowohl $\text{ggT}(a, c) \mid \text{ggT}(a, c \cdot b)$ als auch $\text{ggT}(a, c \cdot b) \mid \text{ggT}(a, c)$ gilt. Da beides Elemente aus \mathbb{N} sind, folgt daraus die Gleichheit $\text{ggT}(a, c) = \text{ggT}(a, c \cdot b)$.

Zur ersten Teilbarkeitsrelation: Wir benutzen zweimal das Lemma von Bézout. Damit existieren ganze Zahlen x und y , so dass

$$\text{ggT}(a, c \cdot b) = a \cdot x + (c \cdot b) \cdot y = a \cdot x + c \cdot \underbrace{(b \cdot y)}_{\in \mathbb{Z}}.$$

Wieder mit dem Lemma von Bézout erhalten wir, dass $\text{ggT}(a, c) \mid \text{ggT}(a, c \cdot b)$ gilt.

Zur zweiten Teilbarkeitsrelation: Wieder folgt alles aus dem Lemma von Bézout. Da a und b teilerfremd sind, gibt es $x, y \in \mathbb{Z}$, mit $1 = a \cdot x + b \cdot y$. Weiter gibt es $x', y' \in \mathbb{Z}$, mit $\text{ggT}(a, c) = a \cdot x' + c \cdot y'$. Damit ist

$$\begin{aligned}
\text{ggT}(a, c) &= (a \cdot x' + c \cdot y') \cdot \underbrace{(a \cdot x + b \cdot y)}_{=1} \\
&= a \cdot \underbrace{(a \cdot x' \cdot x + x' \cdot b \cdot y + c \cdot y' \cdot x)}_{\in \mathbb{Z}} + c \cdot d \cdot \underbrace{(y' \cdot y)}_{\in \mathbb{Z}}.
\end{aligned}$$

Unser lieb gewonnenes Lemma von Bézout liefert nun wie gewünscht $\text{ggT}(a, c \cdot b) \mid \text{ggT}(a, c)$.

Lösung von Aufgabe 67 Es ist

- $24 = 2 \cdot 12 = 2^2 \cdot 6 = 2^3 \cdot 3$
- $60 = 2 \cdot 30 = 2^2 \cdot 15 = 2^2 \cdot 3 \cdot 5$
- $187 = 11 \cdot 17$ (entweder Sie kennen bereits das Resultat aus Aufgabe 70 oder Sie probieren einfach aus 187 durch die Primzahlen 2, 3, 5, ... zu teilen, bis Sie bei 11 einen Treffer gelandet haben)
- $23^5 - 2$ ist ungerade, also nicht durch 2 teilbar. Wir teilen (mit Taschenrechner) $23^5 - 2$ durch 3 und erhalten eine ganze Zahl – also kommt 3 in der Primfaktorisierung von $23^5 - 2$ vor. Das Ergebnis teilen wir wieder durch 3 und erhalten eine ganze Zahl. Diese teilen wir wieder durch 3 und erhalten eine ganze Zahl. Das können wir 10-mal hintereinander machen, also ist 3^{10} ein Teiler von $23^5 - 2$ und

es gilt $23^5 - 2 = 3^{10} \cdot 109$. Da 109 durch keine der Zahlen 2, 3, 5, 7 teilbar ist, muss sie bereits selbst eine Primzahl sein. Damit ist $3^{10} \cdot 109$ die Primfaktorisation von $23^5 - 2$.

Lösung von Aufgabe 68 Sei n keine Primzahl. Falls $n = 1$, so ist $M_n = 2^1 - 1 = 1$ keine Primzahl. Falls $n \neq 1$ ist, gibt es $a, b \in \mathbb{N} \setminus \{1\}$, mit $n = a \cdot b$. Es ist klar, dass damit $M_a \neq M_n$ ist. Die geometrische Reihe (Lemma 3.1) liefert

$$\sum_{i=0}^{b-1} (2^a)^i = \frac{(2^a)^b - 1}{2^a - 1} = \frac{M_n}{M_a} \in \mathbb{N}.$$

Damit ist $M_n \neq M_a \neq 1$ ein Teiler von M_n . Damit kann M_n keine Primzahl sein.

Lösung von Aufgabe 69 Zunächst ganz allgemein: Ist $n \in \mathbb{N}$ mit Primfaktorisation $n = p_1^{e_1} \cdot \dots \cdot p_r^{e_r}$, so gilt

$$\begin{aligned} |\{d \in \mathbb{N} \mid d \mid n\}| &= |\{p_1^{f_1} \cdot \dots \cdot p_r^{f_r} \mid f_i \in \{0, \dots, e_i\} \forall i \in \{1, \dots, r\}\}| \\ &= \left| \prod_{i=1}^r \{0, \dots, e_i\} \right| = \prod_{i=1}^r (e_i + 1). \end{aligned}$$

Zu (a): Wir bestimmen zunächst die Primfaktorisation: $360 = 36 \cdot 10 = 6^2 \cdot 2 \cdot 5 = (2 \cdot 3)^2 \cdot 2 \cdot 5 = 2^3 \cdot 3^2 \cdot 5$. Die Anzahl an Teilern von 360 in \mathbb{N} lässt sich jetzt ganz einfach an den Exponenten ablesen. Es gibt genau $4 \cdot 3 \cdot 2 = 24$ Teiler von 360 in \mathbb{N} .

Zu (b): Sei $n \in \mathbb{N}$ mit Primfaktorisation $n = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_r^{e_r}$. Wir überlegen uns zunächst, dass n genau dann eine Quadratzahl ist, wenn alle e_1, \dots, e_r gerade sind: Sind alle Exponenten gerade, so ist $\frac{e_1}{2}, \dots, \frac{e_r}{2} \in \mathbb{N}_0$ und damit ist $n = (p_1^{e_1/2} \cdot \dots \cdot p_r^{e_r/2})^2$ eine Quadratzahl. Ist andererseits $n = m^2$ eine Quadratzahl und $m = q_1^{f_1} \cdot \dots \cdot q_s^{f_s}$, dann ist $n = (q_1^{f_1} \cdot \dots \cdot q_s^{f_s})^2 = q_1^{2 \cdot f_1} \cdot \dots \cdot q_s^{2 \cdot f_s}$ und alle Exponenten in der Primfaktorisation von n sind gerade. Jetzt folgt die Aussage ganz schnell. Die Anzahl von Teilern von n in \mathbb{N} ist gleich $(e_1 + 1) \cdot \dots \cdot (e_r + 1)$. Damit ist die Anzahl von Teilern ungerade, genau dann wenn alle Faktoren $(e_1 + 1), \dots, (e_r + 1)$ ungerade sind. Das ist genau dann der Fall, wenn alle Exponenten e_1, \dots, e_r gerade sind. Wie wir zu Beginn eingesehen haben, ist dies genau dann der Fall wenn n eine Quadratzahl ist.

Lösung von Aufgabe 70 Jede natürliche Zahl besitzt eine eindeutige Dezimaldarstellung, damit können wir jedes $a \in \mathbb{N}$ schreiben als $a = \sum_{i=0}^n a_i \cdot 10^i$, mit $a_1, \dots, a_n \in \{0, \dots, 9\}$. Es ist $10 \equiv -1 \pmod{11}$ und damit allgemein $10^i \equiv (-1)^i \pmod{11}$ für alle $i \in \mathbb{N}_0$.

Damit gilt nun

$$\begin{aligned}
11 \mid a &\iff 0 \equiv a \equiv \sum_{i=0}^n a_i \cdot 10^i \pmod{11} \\
&\iff 0 \equiv \sum_{i=0}^n a_i \cdot (-1)^i \pmod{11} \\
&\iff 11 \mid \sum_{i=0}^n a_i \cdot (-1)^i = a_0 - a_1 + a_2 - \dots + (-1)^n \cdot a_n
\end{aligned}$$

Lösung von Aufgabe 71 Egal wie wir die Ziffern von 123456789 anordnen, die Quersumme ist immer 45 – also immer durch 3 teilbar. Damit liefert jede Anordnung der Ziffern eine Zahl, die durch 3 teilbar ist und insbesondere keine Primzahl.

Lösung von Aufgabe 72 Zu (a): Sie können den Beweis von Lemma 5.53 nahezu wortgleich übernehmen. Noch schneller geht es mit folgender Abbildung

$$f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \quad ; \quad [i] \mapsto [k] + [i]$$

Diese Abbildung ist bijektiv, da $[i] \mapsto [i] - [k]$ eine Umkehrabbildung ist. Also ist

$$\mathbb{Z}/n\mathbb{Z} = f(\mathbb{Z}/n\mathbb{Z}) = \{[k], [k+1], \dots, [k+n-1]\}.$$

Zu (b): Wir übernehmen die Identifikation der Wochentage mit den Elementen aus $\mathbb{Z}/7\mathbb{Z}$ aus dem Hinweis. Der 13. Januar ist irgendein Wochentag, den wir x nennen. Da der Januar 31 Tage besitzt, ist der 13. Februar der Wochentag $x + [31] = x + [3]$. Genauso machen wir auch für die anderen Monate weiter. Dabei müssen wir natürlich unterscheiden ob wir in einem Schaltjahr sind oder nicht. Es ergibt sich

Datum	Wochentag (kein Schaltjahr)	Wochentag (Schaltjahr)
13. Januar	x	x
13. Februar	$x + [31] = x + [3]$	$x + [31] = x + [3]$
13. März	$x + [3] + [28] = x + [3]$	$x + [3] + [29] = x + [4]$
13. April	$x + [3] + [31] = x + [6]$	$x + [4] + [31] = x$
13. Mai	$x + [6] + [30] = x + [1]$	$x + [30] = x + [2]$
13. Juni	$x + [1] + [31] = x + [4]$	$x + [2] + [31] = x + [5]$
13. Juli	$x + [4] + [30] = x + [6]$	$x + [5] + [30] = x$
13. August	$x + [6] + [31] = x + [2]$	$x + [31] = x + [3]$
13. September	$x + [2] + [31] = x + [5]$	$x + [3] + [31] = x + [6]$
13. Oktober	$x + [5] + [30] = x$	$x + [6] + [30] = x + [1]$
13. November	$x + [31] = x + [3]$	$x + [1] + [31] = x + [2]$
13. Dezember	$x + [3] + [30] = x + [5]$	$x + [2] + [30] = x + [6]$

Die 13ten eines Monats in einem Jahr sind also genau die Wochentage $x, x + [1], x + [2], x + [3], x + [4], x + [5], x + [6]$. Das sind sieben verschiedene Wochentage (vergleichen Sie das mit Teil (a)). Damit kommt jeder

Wochentag – also auch der Freitag – mindestens einmal im Jahr an einem 13ten eines Monats vor.

Lösung von Aufgabe 73 Wir berechnen die Lösungen ganz direkt.

Zu (a): Es ist $7 = 2^2 + 2^1 + 2^0$. Wir berechnen nun

- $[4]^2 = [16] = [3]$
- $[4]^{2^2} = [3]^2 = [9]$

Dann folgt $[4]^7 = [4]^{2^2} \cdot [4]^2 \cdot [4] = [9] \cdot [3] \cdot [4] = [27] \cdot [4] = [1] \cdot [4] = [4]$.
Damit ist $n = 4$ die kleinste natürliche Zahl mit $[4]^7 = [n]$.

Zu (b): Es ist $21 = 2^4 + 2^2 + 2^0$. Wir berechnen nun

- $[6]^2 = [36]$
- $[6]^{2^2} = [36]^2 = [-3]^3 = [9]$
- $[6]^{2^3} = [9]^2 = [81] = [3]$
- $[6]^{2^4} = [3]^2 = [9]$

Damit ist $[6]^{21} = [6]^{2^4} \cdot [6]^{2^2} \cdot [6] = [9] \cdot [9] \cdot [6] = [3] \cdot [6] = [18]$. Damit ist $n = 18$ die kleinste natürliche Zahl mit $[6]^{21} = [n]$.

Lösung von Aufgabe 74 Wir wissen bereits, dass die Kongruenz $a \cdot x \equiv b \pmod{n}$ (mit gegebenen $a, b, n \in \mathbb{Z}$) genau dann lösbar ist, wenn $\text{ggT}(n, a) \mid b$ gilt. Ist dies der Fall, können wir die Lösung mit dem Lemma von Bézou berechnen.

Zu (a): Wir starten mit dem Euklidischen Algorithmus:

$$93 = 1 \cdot 56 + 37$$

$$56 = 1 \cdot 37 + 19$$

$$37 = 1 \cdot 19 + 18$$

$$19 = 1 \cdot 18 + 1$$

Damit ist $\text{ggT}(93, 56) = 1 \mid 2$ und die Kongruenz ist lösbar. Rückwärtsrechnen liefert

$$\begin{aligned} 1 &= 19 - 18 = 19 - (37 - 19) = 2 \cdot 19 - 37 = 2 \cdot (56 - 37) - 37 \\ &= 2 \cdot 56 - 3 \cdot 37 = 2 \cdot 56 - 3 \cdot (93 - 56) = 2 \cdot 56 - 3 \cdot 93 \end{aligned}$$

Betrachten wir diese Gleichung modulo 93 erhalten wir

$$1 \equiv 2 \cdot 56 - 3 \cdot 93 \equiv 2 \cdot 56 \pmod{93}.$$

Dies multiplizieren wir noch mit 2 und erhalten $2 \equiv 4 \cdot 56 \pmod{93}$ und somit ist $x = 4$ eine Lösung der Kongruenz.

Zu (b): Bevor wir groß anfangen zu rechnen, stellen wir fest, dass 22 und 1212 gerade Zahlen sind. Damit muss auch ihr größter gemeinsamer Teiler gerade sein. Es ist also sicher $\text{ggT}(1212, 22) \nmid 11$ und die Kongruenz ist

nicht lösbar. (Da $2 \mid 1212$ und $11 \mid 1212$, wissen wir sogar $22 \mid 1212$ und somit $\text{ggT}(1212, 22) = 22$.)

Zu (c): Entweder wir rechnen exakt wie in (a), oder wir nähern uns der Lösung erst einmal durch $20 \cdot 14 = 280$. Dies modulo 273 ergibt sofort $20 \cdot 14 \equiv 7 \pmod{273}$. Multiplikation mit 5 liefert nun, $(5 \cdot 20) \cdot 14 \equiv 35 \pmod{273}$ – also die Lösung $x = 5 \cdot 20 = 100$.

Zu (d): Wieder überlegen wir zunächst, ob eine Rechnung denn wirklich nötig ist. Die Zahlen 3456 und 48741 sind beide durch 3 teilbar (Quersumme berechnen). Da dies nicht auf 25 zutrifft, folgt wie in (b), dass die Kongruenz nicht lösbar ist.

Lösung von Aufgabe 75 Zunächst einige Vorüberlegungen. Für $a', n' \in \mathbb{N}$ teilerfremd und $k \in \mathbb{N}$ gilt

$$n' \mid a' \cdot k \iff n' \mid k \quad (1.10)$$

Die Richtung \Leftarrow ist eine elementare Teilbarkeitsregel für die wir $\text{ggT}(a', n') = 1$ gar nicht brauchen. Die andere Richtung folgt entweder aus der eindeutigen Primfaktorisierung (Die Primfaktorisation von n' ist in der von $a' \cdot k$ enthalten, aber es gibt keine Primzahl, die n' und a' teilt. Damit muss die gesamte Primfaktorisation von n' bereits in der von k enthalten sein.) oder mit dem Lemma von Bézout (es gibt $x, y \in \mathbb{Z}$, mit $1 = a' \cdot x + n' \cdot y$ – also gibt es $x, y \in \mathbb{Z}$, mit $k = a' \cdot k \cdot x + n' \cdot k \cdot y$. Aus $n' \mid a' \cdot k$ und $n' \mid n'$ folgt sofort $n' \mid a' \cdot k \cdot x + n' \cdot k \cdot y = k$).

Weiter gilt

$$\frac{n}{\text{ggT}(a, n)} \text{ und } \frac{a}{\text{ggT}(a, n)} \text{ sind teilerfremde natürliche Zahlen.} \quad (1.11)$$

Dass $\frac{n}{\text{ggT}(a, n)}$ und $\frac{a}{\text{ggT}(a, n)}$ natürliche Zahlen sind, ist offensichtlich. Die Teilerfremdheit sehen wir wieder mit dem Lemma von Bézout ein: es gibt $x, y \in \mathbb{Z}$, mit $\text{ggT}(a, n) = a \cdot x + n \cdot y$ – also gibt es $x, y \in \mathbb{Z}$, mit $1 = \frac{a}{\text{ggT}(a, n)} \cdot x + \frac{n}{\text{ggT}(a, n)} \cdot y$. Damit müssen $\frac{n}{\text{ggT}(a, n)}$ und $\frac{a}{\text{ggT}(a, n)}$ teilerfremd sein.

Kommen wir nun endlich zur eigentlichen Aufgabe. Seien a, b, n wie in der Aufgabenstellung. Dann gibt es mindestens ein $q \in \mathbb{Z}$ mit $[a] \cdot [q] = [b]$ in $\mathbb{Z}/n\mathbb{Z}$. Für $q' \in \mathbb{Z}$ gilt nun

$$\begin{aligned} [a] \cdot [q'] &= [b] \iff [a] \cdot [q'] = [a] \cdot [q] \iff [a] \cdot ([q] - [q']) = [0] \\ &\iff n \mid a \cdot (q - q') \iff \frac{n}{\text{ggT}(a, n)} \mid \frac{a}{\text{ggT}(a, n)} \cdot (q - q') \\ &\stackrel{(1.10)+(1.11)}{\iff} \frac{n}{\text{ggT}(a, n)} \mid q - q' \\ &\iff q' = q - k \cdot \frac{n}{\text{ggT}(a, n)} \text{ für ein } k \in \mathbb{Z} \end{aligned}$$

Die Lösungen von $[a] \cdot [x] = [b]$ sind also exakt die Restklassen aus der Menge $\{[q - k \cdot \frac{n}{\text{ggT}(a, n)}] \mid k \in \mathbb{Z}\}$. Aus

$$[q + (k + \text{ggT}(a, n)) \cdot \frac{n}{\text{ggT}(a, n)}] = [q + k \cdot \frac{n}{\text{ggT}(a, n)} + n] = [q + k \cdot \frac{n}{\text{ggT}(a, n)}]$$

folgt sofort

$$\{[q - k \cdot \frac{n}{\text{ggT}(a, n)}] \mid k \in \mathbb{Z}\} = \{[q], [q + \frac{n}{\text{ggT}(a, n)}], \dots, [q + (\text{ggT}(a, n) - 1) \cdot \frac{n}{\text{ggT}(a, n)}]\}.$$

Offensichtlich sind die Elemente $[q], [q + \frac{n}{\text{ggT}(a, n)}], \dots, [q + (\text{ggT}(a, n) - 1) \cdot \frac{n}{\text{ggT}(a, n)}]$ paarweise verschieden. Damit besitzt die Menge der Lösungen genau $\text{ggT}(a, n)$ verschiedene Elemente. Das war zu zeigen.

Lösung von Aufgabe 76 Sei also $f : R \rightarrow S$ ein Ring-Homomorphismus und $a \in R$ beliebig.

Zu (a): Es gilt $f(a) = f(a + 0) = f(a) + f(0)$. Damit muss $f(0) = 0$ gelten.

Zu (b): Es ist $f(a) + f(-a) = f(a + (-a)) = f(0) = 0$ und somit $f(-a) = -f(a)$.

Zu (c): Wenn f injektiv ist, gibt es höchstens ein Element in R , das von f auf die Null abgebildet wird. Wir wissen seit gerade eben, dass $f(0) = 0$. Damit ist 0 das einzige Element aus R , das von f auf $0 \in S$ abgebildet wird. Also gibt es kein $b \in R \setminus \{0\}$, mit $f(b) = 0$.

Wir nehmen nun an, dass es kein $b \in R \setminus \{0\}$ gibt, mit $f(b) = 0$. Gilt dann $f(c) = f(d)$, mit $c, d \in R$, so ist

$$0 = f(c) - f(d) \stackrel{(b)}{=} f(c) + f(-d) = f(c - d).$$

Unsere Voraussetzung liefert nun $c - d = 0$, was nichts anderes als $c = d$ bedeutet. Damit ist f injektiv.

Lösung von Aufgabe 77 Wir betrachten den einfachsten Fall von zwei nicht teilerfremden Zahlen – nämlich $n = k = 2$. In $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ gilt für jedes Element $([a], [b]) + ([a], [b]) = ([0], [0])$. In $\mathbb{Z}/4\mathbb{Z}$ hingegen gilt $[1] + [1] = [2] \neq [0]$. Damit haben wir einen eklatanten Unterschied zwischen den beiden Ringen gefunden. Die Ringe sind also nicht isomorph. Das müssen wir natürlich noch etwas formalisieren:

Angenommen es gäbe einen Ring-Isomorphismus $f : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z}$. Dann ist $f([0]_2, [0]_2) = [0]_4$ (siehe Aufgabe 76). Weiter ist f surjektiv, und somit gilt $f([a]_2, [b]_2) = [1]_4$ für gewisse $a, b \in \{0, 1\}$. Dann folgt allerdings

$$\begin{aligned} [0]_4 &= f([0]_2, [0]_2) = f([a]_2, [b]_2) + ([a]_2, [b]_2) \\ &= f([a]_2, [b]_2) + f([a]_2, [b]_2) = [1]_4 + [1]_4 = [2]_4. \end{aligned}$$

Das ist ein Widerspruch und somit sind die beiden Ringe nicht isomorph.

Lösung von Aufgabe 78 Zu (a): *Induktionsanfang:* Für $r = 2$ ist dies genau die bekannte Aussage des Chinesischen Restsatzes.

Induktionsvoraussetzung: Für beliebiges aber festes $r \in \mathbb{N} \setminus \{1\}$ gelte: Sind n_1, \dots, n_r paarweise teilerfremd, so sind die Ringe $\mathbb{Z}/n_1 \dots n_r \mathbb{Z}$ und $\mathbb{Z}/n_1 \mathbb{Z} \times \dots \times \mathbb{Z}/n_r \mathbb{Z}$ isomorph.

Induktionsschritt: Sei r wie in der Induktionsvoraussetzung und seien n_1, \dots, n_{r+1} paarweise teilerfremd. Falls $\text{ggT}(n_{r+1}, n_1 \cdot \dots \cdot n_r) \neq 1$, so gibt es eine Primzahl p , mit $p \mid n_r$ und $p \mid n_1 \cdot \dots \cdot n_r$. Da p eine Primzahl ist, folgt dann aber, dass p einen der Faktoren n_1, \dots, n_r teilt – sagen wir $p \mid n_i$. Dann ist p ein gemeinsamer Teiler von n_r und n_i , was einen Widerspruch zur Annahme darstellt, dass n_1, \dots, n_{r+1} paarweise teilerfremd sind. Damit sind n_{r+1} und $n_1 \cdot \dots \cdot n_r$ teilerfremd. Mit dem Chinesischen Restsatz erhalten wir einen Ring-Isomorphismus

$$f : \mathbb{Z}/n_1 \cdot \dots \cdot n_{r+1} \mathbb{Z} = \mathbb{Z}/(n_1 \cdot \dots \cdot n_r) \cdot n_{r+1} \mathbb{Z} \longrightarrow \mathbb{Z}/n_1 \cdot \dots \cdot n_r \mathbb{Z} \times \mathbb{Z}/n_{r+1} \mathbb{Z}.$$

Da nach Induktionsvoraussetzung die Ringe $\mathbb{Z}/n_1 \cdot \dots \cdot n_r \mathbb{Z}$ und $\mathbb{Z}/n_1 \mathbb{Z} \times \dots \times \mathbb{Z}/n_r \mathbb{Z}$ isomorph sind, ist $\mathbb{Z}/n_1 \cdot \dots \cdot n_{r+1} \mathbb{Z}$ isomorph zu $(\mathbb{Z}/n_1 \mathbb{Z} \times \dots \times \mathbb{Z}/n_r \mathbb{Z}) \times \mathbb{Z}/n_{r+1} \mathbb{Z} = \mathbb{Z}/n_1 \mathbb{Z} \times \dots \times \mathbb{Z}/n_{r+1} \mathbb{Z}$. Das war zu zeigen.

(Hier haben wir folgende wenig überraschende Aussage benutzt: Sind S, S', R Ringe, wobei S und S' isomorph sind, so ist $S \times R$ isomorph zu $S' \times R$. Das wollen wir noch kurz beweisen.

Es gibt also einen Isomorphismus $f : S \longrightarrow S'$. Wir betrachten die Abbildung

$$f' : S \times R \longrightarrow S' \times R \quad ; \quad (s, r) \mapsto (f(s), r).$$

Diese ist unser gewünschter Ring-Isomorphismus, denn für $s_1, s_2 \in S$ und $r_1, r_2 \in R$ gilt

- $f'((s_1, r_1)) + f'((s_2, r_2)) = (f(s_1), r_1) + (f(s_2), r_2) = (f(s_1) + f(s_2), r_1 + r_2) = (f(s_1 + s_2), r_1 + r_2) = f'((s_1 + s_2, r_1 + r_2)) = f'((s_1, r_1) + (s_2, r_2))$
- ganz genauso folgt $f'((s_1, r_1)) \cdot f'((s_2, r_2)) = f'((s_1, r_1) \cdot (s_2, r_2))$
- $f'((1, 1)) = (f(1), 1) = (1, 1)$ (bisjetzt haben wir eingesehen, dass f' ein Ring-Homomorphismus ist).
- Es existiert die Umkehrabbildung f^{-1} von f . Damit existiert auch die Abbildung von $S' \times R$ nach $S \times R$, die durch $(s', r) \mapsto (f^{-1}(s'), r)$ definiert ist. Diese ist offensichtlich eine Umkehrabbildung von f' und ein Ring-Homomorphismus, da f^{-1} einer ist.

Damit ist f' ein Ring-Isomorphismus und $S \times R$ und $S' \times R$ sind isomorph.)

Zu (b): Wir lösen die Aufgaben nacheinander.

- (i) Da $\text{ggT}(5, 7) = 1$, gibt es sicher eine gemeinsame Lösung der beiden Kongruenzen. Durch „scharfes Hinschauen“ sieht man auch recht schnell, dass $x = -2$ eine geeignete Wahl ist. Wer das nicht sieht, kann folgendermaßen eine Lösung berechnen: Es ist $1 = 3 \cdot 5 - 2 \cdot 7$. Damit ist $3 \cdot (-2 \cdot 7) + 5 \cdot (3 \cdot 5) = -42 + 75 = 33$ eine gemeinsame Lösung der Kongruenzen.
- (ii) Wieder folgt aus $\text{ggT}(9, 23) = 1$, dass es eine gemeinsame Lösung geben muss. Es ist $1 = 2 \cdot 23 - 5 \cdot 9$. Damit ist eine gemeinsame Lösung der Kongruenzen gegeben durch $3 \cdot (2 \cdot 23) + 16 \cdot (-5 \cdot 9) = -582$.

- (iii) Es soll $x \equiv 2 \pmod{12}$ gelten. Das geht nur wenn x gerade ist. Gleichzeitig soll auch $x \equiv 7 \pmod{8}$ gelten, was nur für ungerades x möglich ist. Damit können schon die ersten beiden Kongruenzen keine gemeinsame Lösung haben. Es gibt also erst recht kein x , das alle drei Kongruenzen löst.
- (iv) Die Zahlen 3, 5, 8 sind paarweise teilerfremd. Damit folgt aus Teil (a), dass es eine gemeinsame Lösung der drei Kongruenzen gibt. Wir betrachten zunächst nur die ersten beiden Kongruenzen

$$x \equiv 1 \pmod{3} \quad \text{und} \quad x \equiv 2 \pmod{5}.$$

Sei

$$f : \mathbb{Z}/15\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \quad ; \quad [a]_{15} \mapsto ([a]_3, [a]_5)$$

der Ring-Isomorphismus aus dem Chinesischen Restsatz. Dann ist x eine gemeinsame Lösung der beiden Kongruenzen, genau dann wenn $f([x]_{15}) = ([1]_3, [2]_5)$ gilt. Wir sehen (oder berechnen wie in (a)), dass $x = 7$ eine Lösung ist. Damit folgt (aus der Injektivität von f)

$$\begin{aligned} x \equiv 1 \pmod{3} \quad \text{und} \quad x \equiv 2 \pmod{5} &\iff x \in [7]_{15} \\ &\iff x \equiv 7 \pmod{15}. \end{aligned}$$

Jetzt haben wir drei Kongruenzen zu zweien zusammengefasst und es bleibt eine gemeinsame Lösung von

$$x \equiv 7 \pmod{15} \quad \text{und} \quad x \equiv 3 \pmod{8}$$

zu finden. Das machen wir wie immer: Es ist $1 = 2 \cdot 8 - 15$ und damit ist eine gemeinsame Lösung gegeben durch $7 \cdot (2 \cdot 8) + 3 \cdot (-15) = 67$.

Lösung von Aufgabe 79 Sei g die Anzahl von Goldbarren. Aus der Aufgabenstellung entnehmen wir, dass g die folgenden Eigenschaften besitzt:

- $g \equiv 5 \pmod{40}$
- $g \equiv 2 \pmod{7}$
- $0 \leq g \leq 300$

Wir kümmern uns zunächst nur um die ersten beiden Punkte. Wir berechnen wieder (mit dem Euklidischem Algorithmus) $1 = 3 \cdot 40 - 17 \cdot 7$. Damit erfüllt $5 \cdot (-17 \cdot 7) + 2 \cdot (3 \cdot 40) = -355$ die Kongruenzen $-355 \equiv 5 \pmod{40}$ und $-355 \equiv 2 \pmod{7}$. Mit dem Ring-Isomorphismus

$$f : \mathbb{Z}/280\mathbb{Z} \longrightarrow \mathbb{Z}/40\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \quad ; \quad [a]_{280} \mapsto ([a]_{40}, [a]_7)$$

bedeutet dies gerade $f([-355]_{280}) = ([5]_{40}, [2]_7)$. Nach Voraussetzung ist damit $f([g]_{280}) = f([-355]_{280})$. Das ist durch die Injektivität von f äquivalent zu $[g]_{280} = [-355]_{280}$, was nichts anderes als

$$g \in [-355]_{280} = \{\dots, -355, \underbrace{-355 + 280}_{=-75}, \underbrace{-355 + 2 \cdot 280}_{=205}, \underbrace{-355 + 3 \cdot 280}_{=485}, \dots\}$$

bedeutet. Aus $0 \leq g \leq 300$ folgt somit $g = 205$.

Lösung von Aufgabe 80 Sei φ die Eulersche Phi-Funktion.

Zu (a): Wir berechnen als erstes $\varphi(1)$. Dazu müssen wir die Elemente aus $(\mathbb{Z}/1\mathbb{Z})^*$ zählen. Für $a, b \in \mathbb{Z}$ ist $[a]_1 = [b]_1$, genau dann wenn $1 \mid a - b$. Das ist aber immer erfüllt und somit ist $\mathbb{Z}/1\mathbb{Z} = \{[a]_1\}$ für jedes $a \in \mathbb{Z}$. (Insbesondere ist damit $[0]_1 = [1]_1$. Das Einselement und das Nullelement sind somit identisch!). Aus $[1]_1 \cdot [1]_1 = [1]_1$ folgt, dass das einzige Element in $\mathbb{Z}/1\mathbb{Z}$ eine Einheit ist. Damit ist $\varphi(1) = |(\mathbb{Z}/1\mathbb{Z})^*| = 1$.

Für die anderen Werte von φ haben wir eine Formel zur Berechnung. Es ist

- $\varphi(121) = \varphi(11^2) = 11 \cdot 10 = 110$
- $\varphi(2025) = \varphi(5 \cdot 405) = \varphi(5^2 \cdot 81) = \varphi(3^4 \cdot 5^2) = 3^3 \cdot 2 \cdot 5 \cdot 4 = 1080$
- $\varphi(120) = \varphi(2^3 \cdot 3 \cdot 5) = 2^2 \cdot 1 \cdot 2 \cdot 4 = 32$

Zu (b): Sei $n = p_1^{e_1} \cdot \dots \cdot p_r^{e_r}$ die Primfaktorisation von n mit $e_1, \dots, e_r \in \mathbb{N}$. Es soll gelten $\varphi(n) = 6$. Dies ist genau dann der Fall wenn

$$p_1^{e_1-1} \cdot (p_1 - 1) \cdot \dots \cdot p_r^{e_r-1} \cdot (p_r - 1) = 6.$$

Damit gilt $p_i \leq 7$ für alle $i \in \{1, \dots, r\}$, und es ist $n = 2^{e_2} \cdot 3^{e_3} \cdot 5^{e_5} \cdot 7^{e_7}$, wobei die Exponenten nun auch 0 sein dürfen. Falls $e_5 \neq 0$, so ist $4 \mid \varphi(n)$ und somit $\varphi(n) \neq 6$. Damit ist $n = 2^{e_2} \cdot 3^{e_3} \cdot 7^{e_7}$. Falls $e_7 \geq 2$ ist, so ist $7 \mid \varphi(n)$, was ebenfalls $\varphi(n) = 6$ widerspricht. Falls $e_7 = 1$, so ist $6 = \varphi(n) = \varphi(2^{e_2} \cdot 3^{e_3}) \cdot 6$, woraus sofort $n = 7$ oder $n = 14$ folgt. Falls $e_7 = 0$ so gilt $n = 2^{e_2} \cdot 3^{e_3}$ und somit $6 = \varphi(n) = \varphi(2^{e_2}) \cdot \varphi(3^{e_3})$. Um den Faktor 3 in $\varphi(n)$ genau einmal zu erhalten, muss $e_3 = 2$ sein. Damit ist $n = 2^{e_2} \cdot 3^2$. Damit folgt $n = 9$ oder $n = 18$. Fassen wir alles zusammen erhalten wir, dass genau die Elemente $n \in \{7, 14, 9, 18\}$ die Gleichung $\varphi(n) = 6$ erfüllen.

Zu (c): Es ist $\varphi(1) = \varphi(2) = 1$ ungerade. Damit bleibt nur noch zu zeigen, dass $\varphi(n)$ gerade ist für alle $n \in \mathbb{N} \setminus \{1, 2\}$. Für $n = 2^e \in \mathbb{N} \setminus \{1, 2\}$ ist $e \geq 2$ und somit $\varphi(n) = \varphi(2^e) = 2^{e-1}$ eine gerade Zahl. Wenn n nicht von der Form 2^e ist, gibt es eine ungerade Primzahl p , mit $p \mid n$. Dann kommt p in der Primfaktorisation von n vor. Insbesondere gibt es $e \in \mathbb{N}$ und $n' \in \mathbb{N}$, so dass $n = p^e \cdot n'$ und $\text{ggT}(p^e, n') = 1$ gilt. Damit ist

$$\varphi(n) = \varphi(p^e) \cdot \varphi(n') = p^{e-1} \cdot \underbrace{(p-1)}_{\text{gerade}} \cdot \varphi(n')$$

eine gerade Zahl.

Lösung von Aufgabe 81 Wieder ist φ die Eulersche Phi-Funktion.

Zu (a): Dies ist nur eine Umformulierung der bekannten Formel zur Berechnung von $\varphi(n)$. Ist $n = \prod_{i=1}^r p_i^{e_i}$ die Primfaktorisation von n , so ist

$$\begin{aligned} n \cdot \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) &= \prod_{i=1}^r p_i^{e_i} \cdot \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) \\ &= \prod_{i=1}^r p_i^{e_i} \cdot \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^r p_i^{e_i-1} \cdot (p_i - 1) = \varphi(n). \end{aligned}$$

Zu (b): Wir können nun $\varphi(n)$ berechnen nur mit Hilfe der Primzahlen, die n teilen (ohne uns genau darum zu kümmern, mit welcher Potenz sie n teilen). Für jedes $n \in \mathbb{N}$ sei P_n die Menge von Primzahlen p , mit $p \mid n$. Damit können wir nun $\varphi(n) = n \cdot \prod_{p \in P_n} \left(1 - \frac{1}{p}\right)$ schreiben.

Da der ggT von zwei Zahlen genau von den gemeinsamen Primteilern der Zahlen geteilt wird, gilt $P_a \cap P_b = P_{\text{ggT}(a,b)}$. Es folgt $P_{a \cdot b} = P_a \cup (P_b \setminus P_{\text{ggT}(a,b)})$, wobei die beiden Mengen auf der rechten Seite offensichtlich disjunkt sind. Fassen wir das nun alles zusammen erhalten wir

$$\begin{aligned} \varphi(a \cdot b) &= a \cdot b \cdot \prod_{p \in P_{a \cdot b}} \left(1 - \frac{1}{p}\right) = a \cdot b \cdot \prod_{p \in P_a \cup (P_b \setminus P_{\text{ggT}(a,b)})} \left(1 - \frac{1}{p}\right) \\ &= a \cdot b \cdot \prod_{p \in P_a} \left(1 - \frac{1}{p}\right) \cdot \prod_{p \in P_b \setminus P_{\text{ggT}(a,b)}} \left(1 - \frac{1}{p}\right) \\ &= \underbrace{a \cdot \prod_{p \in P_a} \left(1 - \frac{1}{p}\right)}_{=\varphi(a)} \cdot \underbrace{b \cdot \prod_{p \in P_b} \left(1 - \frac{1}{p}\right)}_{=\varphi(b)} \cdot \left(\prod_{p \in P_{\text{ggT}(a,b)}} \left(1 - \frac{1}{p}\right) \right)^{-1} \\ &= \varphi(a) \cdot \varphi(b) \cdot \frac{\text{ggT}(a,b)}{\text{ggT}(a,b) \cdot \prod_{p \in P_{\text{ggT}(a,b)}} \left(1 - \frac{1}{p}\right)} \\ &= \varphi(a) \cdot \varphi(b) \cdot \frac{\text{ggT}(a,b)}{\varphi(\text{ggT}(a,b))}. \end{aligned}$$

Lösung von Aufgabe 82 Zu (a): Seien $n, k, P \in \mathbb{N}$ und $a \in \mathbb{Z}$, mit $\text{ggT}(n, k) = \text{ggT}(a, n \cdot k) = 1$, $\varphi(n) \mid P$ und $\varphi(k) \mid P$. Als erstes stellen wir fest, dass auch $\text{ggT}(a, n) = 1$ ist, da jeder gemeinsame Teiler von a und n erst recht ein gemeinsamer Teiler von a und $n \cdot k$ ist.

Weiter gibt es nach Voraussetzung ein $n' \in \mathbb{N}$ mit $n' \cdot \varphi(n) = P$. Mit dem Satz von Euler erhalten wir damit

$$a^P \equiv a^{\varphi(n) \cdot n'} \equiv (a^{\varphi(n)})^{n'} \equiv 1^{n'} \equiv 1 \pmod{n}.$$

Genauso folgt auch $a^P \equiv 1 \pmod{k}$. Damit ist

$$n \mid a^P - 1 \quad \text{und} \quad k \mid a^P - 1.$$

Da n und k teilerfremd sind folgt daraus $n \cdot k \mid a^P - 1$, was nichts anders bedeutet als $a^P \equiv 1 \pmod{n \cdot k}$.

Zu (b): Wir wenden einfach Teil (a) an. Es ist $100 = 4 \cdot 25$ und $\text{ggT}(4, 25) = 1$. Weiter ist $\varphi(4) = 2$ und $\varphi(25) = 20$. Damit ist also 20 ein gemeinsames Vielfaches von $\varphi(a)$ und $\varphi(25)$ und es folgt aus (a), dass für alle $a \in \mathbb{Z}$ mit $\text{ggT}(a, 100) = 1$ gilt $a^{20} \equiv 1 \pmod{4 \cdot 25}$.

Zu (c): Die letzten beiden Ziffern von 86421^{42124} sind gleich $(86421^{42124} \pmod{100})$. Diese Zahl muss natürlich noch berechnet werden. Offensichtlich ist $42124 = 20 \cdot k + 4$ für eine natürliche Zahl k . Es folgt

$$86421^{42124} \equiv 21^{42124} \equiv 21^{20 \cdot k + 4} \pmod{100} \equiv (21^{20})^k \cdot 21^4 \stackrel{(a)}{\equiv} 21^4 \pmod{100}.$$

Es genügt also $(21^4 \pmod{100})$ zu berechnen:

- $21^2 \equiv (20 + 1)^2 \equiv 400 + 40 + 1 \equiv 41 \pmod{100}$
- $21^4 \equiv 41^2 \equiv 81 \pmod{100}$

Damit endet 86421^{42124} mit den beiden Ziffern 81.

Lösung von Aufgabe 83 Wir müssen zwei Richtungen beweisen.

\Rightarrow Sei nun p eine Primzahl. Wir möchten $[(p-1)!] = [1] \cdot [2] \cdot \dots \cdot [p-1]$ in $\mathbb{Z}/p\mathbb{Z}$ berechnen. Da $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, ist das genau das Produkt über alle Elemente aus $(\mathbb{Z}/p\mathbb{Z})^*$. Sei $[a] \in (\mathbb{Z}/p\mathbb{Z})^*$ mit $[a]^{-1} \neq [a]$. Dann kommt in dem Produkt über alle Einheiten einmal der Faktor $[a]$ und einmal der Faktor $[a]^{-1}$ vor. Diese beiden Faktoren ergeben zusammen natürlich $[1]$. Es ist also $[(p-1)!]$ gleich dem Produkt aller Elemente $[a]$ aus $(\mathbb{Z}/p\mathbb{Z})^*$ mit der Eigenschaft $[a] = [a]^{-1}$. Nun ist

$$\begin{aligned} [a] = [a]^{-1} &\iff [a]^2 = [1] \iff p \mid a^2 - 1 = (a-1) \cdot (a+1) \\ &\iff p \mid a-1 \text{ oder } p \mid a+1 \\ &\iff [a] = [1] \text{ oder } [a] = [-1] = [p-1] \end{aligned}$$

Es folgt $[(p-1)!] = [1] \cdot [2] \cdot \dots \cdot [p-1] = [1] \cdot [p-1] = [p-1] = [-1]$, was nichts anderes bedeutet als $(p-1)! \equiv -1 \pmod{p}$.

\Leftarrow Wir müssen zeigen, dass aus $(p-1)! \equiv -1 \pmod{p}$ bereits folgt, dass p eine Primzahl ist. Wir zeigen die dazu äquivalente Aussage, dass falls p keine Primzahl ist, auch nicht $(p-1)! \equiv -1 \pmod{p}$ gilt.

Sei also $p \in \mathbb{N} \setminus \{1\}$ keine Primzahl. Wir betrachten zunächst den Fall $p = 4$ und erhalten wie gewünscht $(p-1)! = 6 \not\equiv 1 \pmod{p}$. Wir dürfen also im folgenden $p \neq 4$ annehmen.

Wir unterscheiden zwei Fälle. Falls es verschiedene natürliche Zahlen $a, b \in \{1, \dots, p-1\}$ gibt mit $a \cdot b = p$, so ist $p \mid 1 \cdot 2 \cdot \dots \cdot (p-1) = (p-1)!$ und insbesondere ist $(p-1)! \equiv 0 \not\equiv -1 \pmod{p}$.

Falls es keine verschiedenen natürlichen Zahlen $a, b \in \{1, \dots, p-1\}$ gibt mit $a \cdot b = p$, so ist $p = q^2$ für eine Primzahl q . Da wir $p \neq 4$ annehmen, ist $q \geq 3$ und $2 \cdot q < p$. Damit ist $(p-1)! = 1 \cdot 2 \cdot \dots \cdot q \cdot \dots \cdot (2q) \cdot \dots \cdot (p-1)$. Insbesondere ist also $p = q^2 \mid (p-1)!$ und $(p-1)! \equiv 0 \not\equiv -1 \pmod{p}$. Damit ist tatsächlich $(p-1)! \not\equiv -1 \pmod{p}$ für alle zusammengesetzten $p \in \mathbb{N}$.

Lösung von Aufgabe 84 Das Inverse von $[a]$ in $\mathbb{Z}/p\mathbb{Z}$ zu berechnen ist das gleiche wie die Kongruenz $a \cdot x \equiv 1 \pmod{p}$ zu berechnen.

Zu (a): Es ist $2 \cdot 8 = 16 \equiv -1 \pmod{17}$. Damit ist $(-2) \cdot 8 \equiv 1 \pmod{17}$ und $[8]^{-1} = [-2] = [15]$.

Zu (b): Mit dem Euklidischen Algorithmus erhalten wir

$$43 = 8 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

und somit

$$1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5 = 2 \cdot (43 - 8 \cdot 5) - 5 = 2 \cdot 43 - 17 \cdot 5.$$

Es folgt $1 \equiv -17 \cdot 5 \pmod{43}$ und damit ist $[-17] = [26]$ das multiplikative Inverse von $[5]$.

Zu (c): Wieder mit Euklidischem Algorithmus erhalten wir $1 = 5 \cdot 101 - 42 \cdot 12$. Damit ist $1 \equiv -42 \cdot 12 \pmod{101}$ und es gilt $[12]^{-1} = [-42] = [59]$.

Lösung von Aufgabe 85 Es ist $11 \mid 2^{1149} - 6$ genau dann wenn $2^{1146} \equiv 6 \pmod{11}$. Wir müssen also 2^{1149} modulo 11 rechnen. Da $11 \nmid 2$ (und 11 eine Primzahl ist), folgt mit dem kleinen Satz von Fermat

$$2^{1149} \equiv (2^{10})^{114} \cdot 2^9 \equiv 1^{114} \cdot 2^9 \equiv 2^9 \pmod{11}.$$

Aus $2^4 \equiv 16 \equiv 5 \pmod{11}$ folgt $2^8 \equiv 5^2 \equiv 25 \equiv 3 \pmod{11}$. Damit ist nun $2^9 \equiv 3 \cdot 2 \equiv 6 \pmod{11}$. Mit unseren Vorüberlegungen folgt sofort $11 \mid 2^{1149} - 6$.

Dies war die Lösung die für alle solche Aufgabenstellungen funktioniert. Etwas direkter geht es in diesem Fall wenn man aus dem kleinen Satz von Fermat sofort $2^{1150} \equiv 1 \pmod{11}$ – also $11 \mid 2^{1150} - 12 = 2 \cdot (2^{1149} - 6)$ – folgert. Aus $\text{ggT}(2, 11) = 1$, folgt dann bereits $11 \mid 2^{1149} - 6$.

Lösung von Aufgabe 86 Zu (a): Wir betreiben also Polynomdivision im Polynomring $\mathbb{Z}/5\mathbb{Z}[x]$.

(i) Wir berechnen

$$f_1(x) = f(x) - [2] \cdot x^2 \cdot g(x) = [4] \cdot x^4 + [3] \cdot x^3 + [2] \cdot x^2 + x + [2]$$

Das Monom $[2] \cdot x^2$ wurde gewählt, damit der Grad von f_1 echt kleiner ist als der von f . Aus dem gleichen Grund wählen wir als nächstes $[4] \cdot x$ und berechnen

$$f_2(x) = f_1(x) - [4] \cdot x \cdot g(x) = [2]$$

Das ist ein Polynom vom Grad $< \text{grad}(g)$ und wir können aufhören.
Wir setzen die erste Gleichung in die zweite ein und erhalten:

$$\begin{aligned} [2] &= f_2(x) = f_1(x) - [4] \cdot x \cdot g(x) = (f(x) - [2] \cdot x^2 \cdot g(x)) - [4] \cdot x \cdot g(x) \\ &= f(x) - ([2] \cdot x^2 + [4] \cdot x) \cdot g(x) \end{aligned}$$

Damit sind $q(x) = [2] \cdot x^2 + [4] \cdot x$ und $r(x) = f_3(x) = [2]$ die gesuchten Polynome.

(ii) Wir machen das gleiche wie in (i):

$$\begin{aligned} f_1(x) &= f(x) - [4] \cdot x^3 \cdot g(x) = [4] \cdot x^4 + 3 \cdot x^3 + [2] \cdot x^2 + [4] \cdot x + [1] \\ f_2(x) &= f_1(x) - [2] \cdot x^2 \cdot g(x) = [4] \cdot x^3 + x^2 + [4] \cdot x + [1] \\ f_3(x) &= f_2(x) - [2] \cdot x \cdot g(x) = [2] \cdot x^2 + [3] \cdot x + 1 \\ f_4(x) &= f_3(x) - [1] \cdot g(x) = x + [3] \end{aligned}$$

Setzen wir diese Gleichungen sukzessive in einander ein, erhalten wir

$$f_4(x) = f(x) - ([4] \cdot x^3 + [2] \cdot x^2 + [2] \cdot x + [1]) \cdot g(x).$$

Damit sind $q(x) = [4] \cdot x^3 + [2] \cdot x^2 + [2] \cdot x + [1]$ und $r(x) = f_4(x)$ die gesuchten Polynome.

Zu (b): Wir setzen $f(x) = x^4 + [6] \cdot x^3 + [6] \cdot x^2 + [4] \cdot x + [4]$. Nun überprüfen wir für jedes der Elemente aus $\mathbb{Z}/7\mathbb{Z} = \{[0], [1], \dots, [6]\}$ ob es eine Nullstelle von f ist oder nicht.

- $f([0]) = [4] \Rightarrow [0]$ ist keine Nullstelle
- $f([1]) = [0] \Rightarrow [1]$ ist eine Nullstelle
- $f([2]) = [2] \Rightarrow [2]$ ist keine Nullstelle
- $f([3]) = [5] \Rightarrow [3]$ ist keine Nullstelle
- $f([4]) = [0] \Rightarrow [4]$ ist eine Nullstelle
- $f([5]) = [2] \Rightarrow [5]$ ist keine Nullstelle
- $f([6]) = f([-1]) = [1] \Rightarrow [6]$ ist keine Nullstelle

Damit sind $[1]$ und $[4]$ alle Nullstellen von $f(x)$ in $\mathbb{Z}/7\mathbb{Z}$.

Zu (c): Wir können genau das gleiche machen wie in (b). Es gibt aber einen schönen Trick, der uns das Rechnen erspart. Es gilt nämlich

$$(x - [1]) \cdot (x^6 + x^5 + x^4 + x^3 + x^2 + x + [1]) = x^7 - [1].$$

Der kleine Satz von Fermat sagt uns, dass jedes Element aus $\mathbb{Z}/7\mathbb{Z} \setminus \{[0]\}$ eine Nullstelle von $x^7 - [1]$ ist. Damit ist auch jedes Element aus $\mathbb{Z}/7\mathbb{Z} \setminus \{[0]\}$ eine Nullstelle von $(x - [1]) \cdot (x^6 + x^5 + x^4 + x^3 + x^2 + x + [1])$. Aus $[a] - [1] \neq [0]$ für alle $[a] \neq [1]$, folgt sofort, dass jedes Element aus

$\mathbb{Z}/7\mathbb{Z} \setminus \{[0], [1]\}$ eine Nullstelle von $x^6 + x^5 + x^4 + x^3 + x^2 + x + [1]$ ist. Natürlich ist aber auch $[1]$ eine Nullstelle. Wir haben gezeigt, dass die Nullstellen von $x^6 + x^5 + x^4 + x^3 + x^2 + x + [1]$ genau die Elemente aus $\mathbb{Z}/7\mathbb{Z} \setminus \{[0]\}$ sind.

Lösung von Aufgabe 87 Gesucht ist das kleinste $k \in \mathbb{N}$ mit $7 \mid (10^k - 1)$ – also das kleinste $k \in \mathbb{N}$ mit $10^k \equiv 3^k \equiv 1 \pmod{7}$. Es ist also die Ordnung von $[3]$ in $\mathbb{Z}/7\mathbb{Z}$ gesucht. Mit dem kleinen Satz von Fermat wissen wir, dass $[3]^6 = [1]$ ist. Die Ordnung von $[3]$ muss also ein Teiler von 6 sein. Wir überprüfen

- $[3]^1 \neq [1]$
- $[3]^2 = [9] = [2] \neq [1]$
- $[3]^3 = [3]^2 \cdot [3] = [2] \cdot [3] = [6] = [-1] \neq [1]$.

Der einzige Teiler der 6, der noch übrigbleibt, ist die 6 selbst. Damit ist die gesuchte Zahl $k = 6$. (Das bedeutet, dass $[3] = [10]$ ein erzeugendes Element von $(\mathbb{Z}/7\mathbb{Z})^*$ ist.)

Lösung von Aufgabe 88 Sei $g \in G$ beliebig. Dann ist $g^{\text{ord}(g)-1} \cdot g = g^{\text{ord}(g)} = e$ und somit $g^{-1} = g^{\text{ord}(g)-1}$. Dann ist für jedes $k \in \mathbb{N}$

$$\begin{aligned} g^k = e &\iff (g^k) \cdot (g^{-1})^k = e \cdot (g^{-1})^k \iff g^{k+(\text{ord}(g)-1) \cdot k} = (g^{-1})^k \\ &\iff (g^{\text{ord}(g)})^k = (g^{-1})^k \iff e = (g^{-1})^k \end{aligned}$$

Insbesondere ist $(g^{-1})^{\text{ord}(g)} = e = g^{\text{ord}(g)}$ und $(g^{-1})^k \neq e \neq g^{\text{ord}(g)}$ für alle $k \in \{1, \dots, \text{ord}(g)-1\}$. Damit ist $\text{ord}(g)$ die kleinste natürliche Zahl mit $(g^{-1})^{\text{ord}(g)} = e$, was nichts anderes bedeutet als $\text{ord}(g) = \text{ord}(g^{-1})$.

Lösung von Aufgabe 89 Zu (a): Es ist $(\mathbb{Z}/4\mathbb{Z})^* = \{[1], [3]\} = \{[3], [3]^2\}$. Also ist $(\mathbb{Z}/4\mathbb{Z})^*$ zyklisch.

Nun betrachten wir $(\mathbb{Z}/8\mathbb{Z})^* = \{[1], [3], [5], [7]\}$. Wir wissen bereits, dass das Quadrat einer ungeraden Zahl kongruent zu 1 modulo 8 ist. Damit besitzt jedes Element aus $(\mathbb{Z}/8\mathbb{Z})^*$ höchstens Ordnung 2. Insbesondere ist $(\mathbb{Z}/8\mathbb{Z})^*$ nicht zyklisch.

Zu (b): Wir testen wieder die kleinsten Möglichen Zahlen. Es ist $(\mathbb{Z}/9\mathbb{Z})^* = \{[1], [2], [4], [5], [7], [8]\}$. Wir berechnen die Potenzen von $[2]$ und erhalten $[2]^2 = [4]$, $[2]^3 = [8]$, $[2]^4 = [7]$, $[2]^5 = [5]$ und $[2]^6 = [1]$. Damit ist jedes Element aus $(\mathbb{Z}/9\mathbb{Z})^*$ von der Form $[2]^k$. Insbesondere ist $(\mathbb{Z}/9\mathbb{Z})^*$ zyklisch.

Als nächstes betrachten wir $(\mathbb{Z}/15\mathbb{Z})^*$. Wir könnten wieder die Ordnungen der Elemente berechnen, aber wir haben mittlerweile ja schon einige theoretische Hilfsmittel kennengelernt. Für jede Primzahl p sind die Gruppen $(\mathbb{Z}/p\mathbb{Z})^*$ und $\mathbb{Z}/(p-1)\mathbb{Z}$ isomorph. Damit und mit dem Chinesischen Restsatz folgt nun, dass $(\mathbb{Z}/15\mathbb{Z})^*$ isomorph ist zu $(\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$, also isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. In $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ ist die Ordnung jedes Elementes ein Teiler von 4. Insbesondere gibt es kein Element der Ordnung 8 in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ und somit gibt es kein Element der Ordnung 8 in $(\mathbb{Z}/15\mathbb{Z})^*$. Damit kann $(\mathbb{Z}/15\mathbb{Z})^*$ nicht zyklisch sein.

Lösung von Aufgabe 90 Für $[a] = [0]$ sind offensichtlich beide Aussagen falsch. Wir beweisen die nötigen Implikationen für $[a] \neq [0]$.

\Rightarrow Wir zeigen die äquivalente Aussage, dass $[a] \notin (\mathbb{Z}/n\mathbb{Z})^*$ impliziert, dass $\text{ord}([a]) \neq n$ ist. Wenn $[a] \notin (\mathbb{Z}/n\mathbb{Z})^*$ gilt, so ist $\text{ggT}(a, n) = d \neq n$. Damit sind $\frac{a}{d}$ und $\frac{n}{d}$ natürliche Zahlen und es gilt $1 \leq \frac{n}{d} < n$. Weiter ist

$$\underbrace{[a] + \dots + [a]}_{\frac{n}{d}\text{-mal}} = \underbrace{[a + \dots + a]}_{\frac{n}{d}\text{-mal}} = \left[\frac{n}{d} \cdot a\right] = \left[n \cdot \frac{a}{d}\right] = [0]$$

(hier ist es von entscheidender Bedeutung, dass $\frac{a}{d} \in \mathbb{Z}$ ist!). Damit ist die Ordnung von $[a]$ höchstens $\frac{n}{d}$ und insbesondere ist $\text{ord}([a]) \neq n$.

\Leftarrow Sei nun $[a] \in (\mathbb{Z}/n\mathbb{Z})^*$. Natürlich gilt $\underbrace{[a] + \dots + [a]}_{n\text{-mal}} = [n \cdot a] = [0]$. Insbesondere

ist also $\text{ord}([a]) \mid n$. Andererseits gilt

$$[0] = \underbrace{[a] + \dots + [a]}_{\text{ord}([a])\text{-mal}} = [\text{ord}([a]) \cdot a] = [\text{ord}([a])] \cdot [a].$$

Multiplizieren wir auf beiden Seiten mit $[a]^{-1}$, erhalten wir

$$[0] = [0] \cdot [a]^{-1} = [\text{ord}([a])] \cdot [a] \cdot [a]^{-1} = [\text{ord}([a])],$$

also $n \mid \text{ord}([a])$. Da sowohl n als auch $\text{ord}([a])$ in \mathbb{N} sind, folgt die Gleichheit $n = \text{ord}([a])$.

Lösung von Aufgabe 91 Zu (a): Da p ungerade ist, ist $p - 1$ gerade und $\frac{p-1}{2}$ ist eine natürliche Zahl. Nun ist $([a]^2)^{(p-1)/2} = [a]^{p-1} = [1]$. Insbesondere ist die Ordnung von $[a]^2$ ein Teiler von $\frac{p-1}{2}$ und somit ungleich $p - 1$. Damit ist $[a]^2$ kein erzeugendes Element von $(\mathbb{Z}/p\mathbb{Z})^*$.

Zu (b): Es gibt genau $\varphi(17 - 1) = \varphi(16) = 8$ erzeugenden Elemente von $(\mathbb{Z}/17\mathbb{Z})^*$. Wir benutzen (a) um einige Elemente auszuschließen. Wir wissen nämlich, dass die folgenden Elemente keine erzeugenden Elemente sein können:

$$\begin{aligned} [1]^2 &= [1] & [2]^2 &= [4] & [3]^2 &= [9] & [4]^2 &= [16] \\ [5]^2 &= [8] & [6]^2 &= [2] & [7]^2 &= [15] & [8]^2 &= [13] \end{aligned}$$

Jetzt bleiben nur noch 8 Elemente übrig – nämlich $[3], [5], [6], [7], [10], [11], [12], [14]$. Da wir bereits festgestellt haben, dass es genau 8 erzeugenden Elemente gibt, müssen alle diese Elemente die gesuchten erzeugenden Elemente sein.

Zu (c): Wieder wissen wir, dass es genau $\varphi(19 - 1) = \varphi(18) = 6$ erzeugenden Elemente gibt. Wir berechnen wieder die Quadrate der Elemente um einige Kandidaten auszuschließen:

$$\begin{aligned}
[1]^2 &= [1] \quad , & [2]^2 &= [4] \quad , & [3]^2 &= [9] \quad , & [4]^2 &= [16] \quad , \\
[5]^2 &= [6] \quad , & [6]^2 &= [17] \quad , & [7]^2 &= [11] \quad , & [8]^2 &= [7] \quad , \\
[9]^2 &= [5]
\end{aligned}$$

Mehr Quadrate gibt es nicht, da es nun mit $[10]^2 = [-9]^2 = [9]^2$ weitergehe, was wir schon berechnet haben. Es bleiben noch die Kandidaten

$$[2] \quad [3] \quad [8] \quad [10] \quad [12] \quad [13] \quad [14] \quad [15] \quad [18]$$

übrig, von denen genau 6 erzeugenden Elemente sind. Da $[18] = [-1]$ offensichtlich kein erzeugenden Element ist, müssen wir nur zwei weitere ausschließen. Wir rechnen solange, bis wir auf $[8]^6 = [1]$ stoßen. Damit sind die Elemente $[8]$ und $[8]^{-1} = [12]$ keine erzeugenden Elemente und wir sind fertig: Alle erzeugenden Elemente sind

$$[2] \quad [3] \quad [10] \quad [13] \quad [14] \quad [15] \quad [18]$$

Zu (d): Für jeden Teiler d von $11 - 1 = 10$ gibt es genau $\varphi(d)$ Elemente der Ordnung d . Es gibt also genau ein Element der Ordnung 1 (natürlich das Element $[1]$), genau ein Element der Ordnung 2 (natürlich das Element $[-1] = [10]$), genau vier Elemente der Ordnung 5 und genau vier Elemente der Ordnung 10. Wir müssen also wieder nur noch die erzeugenden Elemente von $(\mathbb{Z}/11\mathbb{Z})^*$ bestimmen:

- $[2]^2 = [4]$ ist kein erzeugenden Element, also gilt $\text{ord}([4]) = 5$
- $[3]^2 = [9]$ ist kein erzeugenden Element, also gilt $\text{ord}([9]) = 5$
- $[4]^2 = [5]$ ist kein erzeugenden Element, also gilt $\text{ord}([5]) = 5$
- $[5]^2 = [3]$ ist kein erzeugenden Element, also gilt $\text{ord}([3]) = 5$

Wir haben also die vier Elemente der Ordnung 5 gefunden und notwendigerweise haben die übrigen Elemente

$$[2] \quad [6] \quad [7] \quad [8]$$

alle die Ordnung 10.

1.6 Lösungen der Aufgaben aus Kapitel 6

Lösung von Aufgabe 92 Dieser Text ist offensichtlich chiffriert. Wir gehen davon aus, dass es sich bei der Chiffre um eine Caesar-Verschlüsselung handelt (bevor wir etwas kompliziertes machen, können wir ja erstmal den einfachsten Fall überprüfen). Weiter wird der Text wahrscheinlich wie der Rest des Buches auf deutsch verfasst sein. Damit gehen wir davon aus, dass der Häufigste Buchstabe der Chiffre, dem Buchstaben E entspricht. Der Buchstabe der in der Chiffre am häufigsten vorkommt,

ist das K (23-mal; auf Platz zwei folgt das O, welches 11-mal vorkommt). Wir gehen also davon aus, dass $E + \text{Schlüssel} = K$ gilt und vermuten somit, dass der Schlüssel gleich $K - E = F$ ist. Wir ziehen also von jedem Buchstaben der Chiffre, den Buchstaben F ab. Dann erhalten wir:

ENTSCHLUESSELN SIE DIE ZWEITE AUFGABE DIE MIT EINER VIGENÈRE VERSCHLUESSELUNG MIT SCHLUESSEL „UNI“ CHIFFRIERT WURDE

Lösung von Aufgabe 93 Wir wissen, dass dies eine Chiffre ist, die durch die Vigenère-Verschlüsselung mit dem Schlüssel UNI erstellt wurde. Wir ziehen also vom ersten Buchstaben den Buchstaben U ab, vom zweiten den Buchstaben N und vom dritten den Buchstaben I. Dann geht es wieder mit U los und so weiter Wir erhalten:

WIE VIELE MONOALPHABETISCHE SUBSTITUTIONEN GIBT ES DIE JEDEM BUCHSTABEN DES ALPHABETS GENAU EINEN BUCHSTABEN ZUORDNEN? BEI WIE VIELEN DIESER SUBSTITUTIONEN WIRD KEIN BUCHSTABE SICH SELBST ZUGEORDNET?

Ach du Schreck! Noch eine Aufgabe! Dass jedem Buchstaben des Alphabets genau ein anderer Buchstabe zugeordnet wird, bedeutet nichts anderes, als dass wir eine bijektive Abbildung von der Menge der Buchstaben nach sich selbst betrachten. Davon gibt es natürlich genau $26!$ viele. Wenn nun kein Buchstabe sich selbst zugeordnet wird, haben wir eine Fixpunktfreie Permutation der Buchstaben. Dies berechnen wir genau wie in Aufgabe 29 mit dem Inklusions-Exklusions Prinzip. Dazu sei Ω die Menge aller Buchstaben und für jedes $\alpha \in \Omega$ definieren wir

$$A_\alpha = \{f \in \text{Bij}(\Omega) \mid f(\alpha) = \alpha\}$$

Wir suchen also genau die Zahl

$$26! - \left| \bigcup_{\alpha \in \Omega} A_\alpha \right|.$$

Für jedes $\alpha \in \Omega$ gilt nun $|A_\alpha| = 25!$. Allgemein gilt: Ist $\Gamma \subseteq \Omega$, mit $|\Gamma| = r$, so ist $\left| \bigcap_{\alpha \in \Gamma} A_\alpha \right| = (26 - r)!$. Da es für jedes $r \in \{1, \dots, 26\}$ genau $\binom{26}{r}$ verschiedene Wahlen Teilmengen $\Gamma \subseteq \Omega$, mit $|\Gamma| = r$, gibt, folgt mit dem Inklusions-Exklusions Prinzip

$$\begin{aligned} 26! - \left| \bigcup_{\alpha \in \Omega} A_\alpha \right| &= 26! - \left(\sum_{r=1}^{26} (-1)^{r+1} \binom{26}{r} \cdot (26 - r)! \right) \\ &= 26! + \left(\sum_{r=1}^{26} (-1)^r \binom{26}{r} \cdot (26 - r)! \right) = \sum_{r=0}^{26} (-1)^r \binom{26}{r} \cdot (26 - r)! \\ &= 26! \cdot \sum_{r=0}^{26} (-1)^r \frac{1}{r!} = 148362637348470135821287825 \end{aligned}$$

Lösung von Aufgabe 94 Wir sehen, dass ganze Wörter gleich verschlüsselt wurden. Der Abstand der Buchstaben aus den beiden YMAXHWG beträgt genau 27, der Abstand zwischen allen Buchstaben aus den beiden GDBFYXO XEJWZFF beträgt genau 21. Wir gehen also davon aus, dass die Schlüssellänge sowohl 27 als auch 21 teilt. Unsere Vermutung ist daher, dass die Schlüssellänge gleich 3 ist. Nun schreiben wir jeden dritten Buchstaben der Chiffre in eine Reihe. Dann erhalten wir die drei Reihen

- OFAWWDYXWFAWDYXWFFJJ (häufigster Buchstabe: W)
- XYXGGKBXEZYXGBXEZAMA (häufigster Buchstabe: X)
- OMHIUGFOJFMHGFOJFJFF (häufigster Buchstabe: F)

Wenn unsere Vermutung stimmt, wurde jeder Buchstabe der ersten Reihe mit dem ersten Buchstaben des Schlüssels chiffriert, jeder Buchstabe der zweiten Reihe, mit dem zweiten Buchstaben des Schlüssels und jeder Buchstabe der dritten Reihe mit dem dritten Buchstaben des Schlüssels.

Wir versuchen also den Schlüssel $(W-E)(X-E)(F-E)=RSA$ (das sieht schon so aus als könnte das richtig sein). Entschlüsseln wir nur die Chiffre mit diesem Schlüssel erhalten wir

WENN FLIEGEN HINTER FLIEGEN FLIEGEN
FLIEGEN FLIEGEN FLIEGEN HINTERHER

Lösung von Aufgabe 95 Wir suchen ein Element $e \in \{1, \dots, 22\}$ mit $[7]^e = [17]$ in $(\mathbb{Z}/23\mathbb{Z})^*$. Uns bleibt nichts anderes als auszuprobieren:

- $[7]^1 = [1] \neq [17]$
- $[7]^2 = [3] \neq [17]$
- $[7]^3 = [21] \neq [17]$
- $[7]^4 = [9] \neq [17]$
- $[7]^5 = [17]$

Damit ist der diskrete Logarithmus von $[17]$ zur Basis $[7]$ gleich 5.

Lösung von Aufgabe 96 Es wird der Schlüssel $(B^a \bmod p) = (13^4 \bmod 29) = 25$ erzeugt.

Lösung von Aufgabe 97 Eine Zahl aus Ω , die auf 0, 2, 4, 6 oder 8 endet ist gerade und somit keine Primzahl. Eine Zahl aus Ω , die auf 5 endet ist durch 5 teilbar und ebenfalls keine Primzahl. Damit gibt es in $\Omega \setminus \Omega'$ keine Primzahlen. Anders formuliert, in Ω' gibt es genauso viele Primzahlen wie in Ω – nämlich ungefähr $\frac{2^{1024}}{\log(2^{1024})} - \frac{2^{1023}}{\log(2^{1023})}$. Allerdings ist $|\Omega'|$ ungefähr gleich $\frac{4}{10} \cdot |\Omega|$, da von 10 aufeinanderfolgenden Zahlen in Ω genau 4 in Ω' sind. Die Wahrscheinlichkeit dafür, dass eine zufällig gewählte Zahl aus Ω' eine Primzahl ist, ist also ungefähr

$$\frac{5}{2} \cdot \frac{\frac{2^{1024}}{\log(2^{1024})} - \frac{2^{1023}}{\log(2^{1023})}}{|\Omega|} = 0.003518 \dots$$

Lösung von Aufgabe 98 Zu (a): Da $r \geq 2$, ist n zusammengesetzt. Sei nun $a \in \mathbb{Z}$, mit $\text{ggT}(a, n) = 1$. Dann gilt für jedes $i \in \{1, \dots, r\}$, dass p_i kein Teiler von a ist. Sei nun $i \in \{1, \dots, r\}$ beliebig. Dann existiert nach Voraussetzung $n_i \in \mathbb{N}$, mit $(p_i - 1) \cdot n_i = n - 1$. Mit dem kleinen Satz von Fermat gilt somit

$$a^{n-1} \equiv (a^{p_i-1})^{n_i} \equiv 1^{n_i} \equiv 1 \pmod{p_i}. \quad (1.12)$$

Damit ist $p_i \mid a^{n-1} - 1$. Insbesondere kommt jede der Primzahlen p_1, \dots, p_r in der Primfaktorisation von $a^{n-1} - 1$ vor. Damit ist $n = p_1 \cdot \dots \cdot p_r \mid a^{n-1} - 1$, was nichts anderes als $a^{n-1} \equiv 1 \pmod{n}$ bedeutet. Da dies für alle $a \in \mathbb{Z}$ gilt, die teilerfremd zu n sind, ist n eine Carmichael-Zahl.

Zu (b): Sei n eine zusammengesetzte gerade Zahl (also insbesondere $n \neq 2$). Dann ist erstens $n \nmid 2$ und somit $-1 \not\equiv 1 \pmod{n}$; und zweitens $(-1)^{n-1} \equiv (-1) \pmod{n}$, da $n - 1$ ungerade ist. Damit erfüllt $a = -1$ die Bedingungen $\text{ggT}(a, n) = 1$ und $a^{n-1} \not\equiv 1 \pmod{n}$. Damit ist n keine Carmichael-Zahl.

Lösung von Aufgabe 99 Die Dechiffrierzahl d erfüllt

$$d \cdot \underbrace{e}_{=100001} \equiv 1 \pmod{\underbrace{p \cdot q}_{\varphi(443 \cdot 467)}},$$

wobei φ die Eulersche-Phi Funktion ist. Es ist $\varphi(443 \cdot 467) = 442 \cdot 466 = 205972$. Mit dem Euklidischen Algorithmus berechnen wir (um die Rechnung zu verkürzen arbeiten wir auch mit negativen Zahlen)

$$\begin{aligned} 205972 &= 2 \cdot 100001 + 5970 \\ 100001 &= 17 \cdot 5970 - 1489 \\ 5970 &= (-4) \cdot (-1489) + 14 \\ -1489 &= (-106) \cdot 14 - 5 \\ 14 &= (-3) \cdot (-5) - 1 \end{aligned}$$

Damit folgt

$$\begin{aligned} 1 &= 3 \cdot 5 - 14 = 3 \cdot (1489 - 106 \cdot 14) - 14 = 3 \cdot 1489 - 319 \cdot 14 \\ &= 3 \cdot 1489 - 319 \cdot (5970 - 4 \cdot 1489) = 1279 \cdot 1489 - 319 \cdot 5970 \\ &= 1279 \cdot (17 \cdot 5970 - 100001) - 319 \cdot 5970 = 21424 \cdot 5970 - 1279 \cdot 100001 \\ &= 21424 \cdot (205972 - 2 \cdot 100001) - 1279 \cdot 100001 \\ &= 21424 \cdot 205972 - 44127 \cdot 100001 \end{aligned}$$

und somit $-44127 \cdot e \equiv 1 \pmod{\varphi(p \cdot q)}$. Wir können für d damit jedes Element aus $[-44127]_{205972}$ wählen. Wir entscheiden uns hier für $d = -44127 + 205972 = 161845$.

Lösung von Aufgabe 100 Es ist $11 = 2^3 + 2 + 1$. Wir berechnen nun

- $(74)^2 \equiv (-3)^2 \equiv 9 \pmod{77}$

- $(74)^4 \equiv 9^2 \equiv 81 \equiv 4 \pmod{77}$
- $(74)^8 \equiv 4^2 \equiv 16 \pmod{77}$

Es folgt $(74)^{11} \equiv (74)^8 \cdot (74)^2 \cdot (74) \equiv 16 \cdot 9 \cdot (-3) \equiv 144 \cdot (-3) \equiv (-10) \cdot (-3) \equiv 30 \pmod{77}$.

Alternativ können Sie auch mit dem kleinen Satz von Fermat $74^{11} \equiv 74 \equiv 8 \pmod{11}$ und $74^{11} \equiv 74^5 \equiv 4^5 \equiv 2 \pmod{7}$ berechnen. Danach berechnet man mit dem Chinesischen Restsatz ein Element x , was $x \equiv 8 \pmod{11}$ und $x \equiv 2 \pmod{7}$ erfüllt. Dieses x ist dann kongruent zu 74^{11} modulo 77.

Lösung von Aufgabe 101 Die Idee ist, dass die „Entschlüsselung“ im RSA-Verfahren nicht nur dann gilt, wenn wir modulo dem Produkt zweier verschiedener Primzahlen rechnen. Ist $d \in \mathbb{N}$ mit $d \cdot 77 \equiv 1 \pmod{\varphi(97)}$, so ist $x^{77 \cdot d} \equiv x \pmod{97}$.

Wir Berechnen also als erstes ein $d \in \mathbb{N}$ mit $d \cdot 77 \equiv 1 \pmod{\varphi(97)}$. Da 97 eine Primzahl ist, ist $\varphi(97) = 96$:

$$\begin{aligned} 96 &= 1 \cdot 77 + 19 \\ 77 &= 4 \cdot 19 + 1 \quad \implies \quad 1 = 5 \cdot 77 - 4 \cdot 96 \end{aligned}$$

Es ist also $5 \cdot 77 \equiv 1 \pmod{\varphi(97)}$ und damit gilt

$$x \equiv x^{77 \cdot 5} \equiv (x^{77})^5 \equiv (4)^5 \pmod{97}.$$

Wir müssen also nur noch $4^5 \pmod{97}$ berechnen:

- $4^2 \equiv 16 \pmod{97}$
- $4^4 \equiv 16^2 \equiv 100 + 120 + 36 \equiv 3 + 23 + 36 \equiv 62 \pmod{97}$
- $4^5 \equiv 62 \cdot 4 \equiv (-35) \cdot 4 \equiv -140 \equiv -43 \equiv 54 \pmod{97}$

Fassen wir alles zusammen erhalten wir, dass $54^{77} \equiv 4 \pmod{97}$ gilt. Damit ist $x = 54$ eine Lösung der Kongruenz.

Lösung von Aufgabe 102 Wir wollen den privaten Schlüssel konstruieren. Dazu müssen wir $N = 221$ faktorisieren. Nach kurzem Überlegen sehen wir $N = 13 \cdot 17$. Damit ist $p = 13$ und $q = 17$ der private Schlüssel. Insbesondere ist $\varphi(N) = 12 \cdot 16 = 192$.

Jetzt können wir die Dechiffrierzahl berechnen. Mit dem Euklidischen Algorithmus erhalten wir $7 \cdot 55 \equiv 1 \pmod{192}$. Damit ist $d = 7$ die Dechiffrierzahl.

Nun entschlüsseln wir den Securecode m . Wir wissen, dass $m^e \equiv c \equiv 94 \pmod{221}$ ist. Damit wissen wir

$$m \equiv (m^e)^d \equiv 94^7 \equiv 172 \pmod{221}.$$

Damit ist Mias Securecode gleich 172.

Lösung von Aufgabe 103 Zu (a): Wir wissen $N = p \cdot q = 53929$ und $\varphi(N) = (p-1) \cdot (q-1) = 53460$. Damit ist $-(p+q) = \varphi(N) - N - 1 = -470$ und p und q sind die Nullstellen von

$$(x - p) \cdot (x - q) = x^2 - 470 \cdot x + 53929.$$

Wir wir diese Nullstellen berechnen wissen wir aus der Schule. Sie sind gegeben durch $235 \pm \sqrt{235^2 - 53929}$ – also durch $p = 271$ und $q = 199$. Damit ist die Faktorisierung $N = 271 \cdot 199$.

Zu (b): Es ist $\sqrt{79523} = 281.998 \dots$. Wir suchen Teiler von 79523 in der Menge $\{1, \dots, 281\}$, wobei wir mit der größten Zahl starten. Wir rechnen $\frac{79523}{281} = 283$ und sind schon fertig. Denn jetzt wissen wir bereits, dass $N = 79523 = 283 \cdot 281$ ist.

1.7 Lösungen der Aufgaben aus Kapitel 7

Lösung von Aufgabe 104 Die Aussage ist eigentlich vollkommen offensichtlich: Wenn wir die Einträge in einem lateinischen Quadrat umbenennen (nichts anderes macht eine bijektive Abbildung), bleibt es immer noch ein lateinisches Quadrat.

Wir argumentieren natürlich auch noch einmal formal. Es ist $\sigma(M_1) = M_2$ (da σ surjektiv ist) und für $m, n \in M_1$ gilt

$$\sigma(m) = \sigma(n) \iff m = n$$

(da σ injektiv ist). Seien nun $i, i', j, j' \in \{1, \dots, n\}$ beliebig, dann ist

$$L^\sigma(i, j) = L^\sigma(i, j') \iff \sigma(L(i, j)) = \sigma(L(i, j')) \iff L(i, j) = L(i, j') \iff j = j'.$$

Genauso folgt auch, dass $L^\sigma(i, j) = L^\sigma(i', j)$ genau dann gilt, wenn $i = i'$. Damit ist L^σ ein lateinisches Quadrat der Ordnung $|\sigma(M_1)| = n$.

Lösung von Aufgabe 105 Die erste Zeile eines lateinischen Quadrates der Ordnung $n \in \mathbb{N}$ mit Einträgen aus $\{1, \dots, n\}$ ist eine Permutation der Elemente aus $\{1, \dots, n\}$. Es gibt also genau $n!$ mögliche erste Zeilen für ein solches lateinisches Quadrat.

Zu (a): Für jede Permutation (m_1, m_2, m_3) der Elemente aus $\{1, 2, 3\}$ gibt es genau zwei lateinische Quadrate mit erster Zeile $m_1 \ m_2 \ m_3$. Nämlich:

$$\begin{array}{cc} m_1 & m_2 & m_3 \\ m_2 & m_3 & m_1 \\ m_3 & m_1 & m_2 \end{array} \quad \text{und} \quad \begin{array}{cc} m_1 & m_2 & m_3 \\ m_3 & m_1 & m_2 \\ m_2 & m_3 & m_1 \end{array}$$

Damit gibt es genau $3! \cdot 2 = 12$ lateinische Quadrate der Ordnung 3 mit Einträgen aus $\{1, 2, 3\}$.

Zu (b): Wir lesen von rechts nach links und von oben nach unten. Dann haben wir für den ersten freien Eintrag 3 Möglichkeiten, nämlich 1, 3 und 4. Jede dieser Wahlen bestimmt die zweite Zeile vollständig. Für die ersten beiden Zeilen gibt es also die Möglichkeiten

$$\text{A: } \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{array} \quad \text{und} \quad \text{B: } \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{array} \quad \text{und} \quad \text{C: } \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{array}$$

In den Fällen B und C ist die dritte Zeile wieder vollständig durch die Wahl des ersten Eintrages bestimmt. Damit gibt es in diesen Fällen nur die Möglichkeiten

1 2 3 4		1 2 3 4		1 2 3 4		1 2 3 4
2 3 4 1	und	2 3 4 1	und	2 4 1 3	und	2 4 1 3
3 4 1 2		4 1 2 3		3 1 4 2		4 3 2 1

Im Fall A bleibt nach dem ersten Eintrag der dritten Zeile immer noch eine Wahlmöglichkeit übrig. Damit gibt es 4 Möglichkeiten in Fall A eine dritte Zeile zu wählen. Nämlich

1 2 3 4		1 2 3 4		1 2 3 4		1 2 3 4
2 1 4 3	und	2 1 4 3	und	2 1 4 3	und	2 1 4 3
3 4 1 2		3 4 2 1		4 3 1 2		4 3 2 1

Natürlich können wir jedes lateinische Quadrat in dem die letzte Zeile fehlt, eindeutig zu einem vollständigen lateinischen Quadrat erweitern. Insbesondere können wir die Tabelle aus der Aufgabenstellung auf genau 8 verschiedene Arten zu einem lateinischen Quadrat vervollständigen.

Zu (c): Für die erste Zeile des lateinischen Quadrates haben wir $4!$ Möglichkeiten. Für den ersten Eintrag der zweiten Zeile haben wir dann 3 Möglichkeiten. Wie wir in (b) gesehen haben, haben wir nach diesen Wahlen noch 8 Möglichkeiten, die Tabelle zu einem lateinischen Quadrat zu vervollständigen. Damit können wir genau $4! \cdot 3 \cdot 8 = 576$ verschiedene lateinische Quadrate der Ordnung 4 mit Einträgen aus $\{1, 2, 3, 4\}$ konstruieren.

Lösung von Aufgabe 106 (i) Ein von 12 möglichen Systemen verschiedener Repräsentanten ist $(5, 2, 1, 4)$.

(ii) Es gibt fünf Mengen, die zusammen nur vier verschiedene Elemente besitzen. Es kann also nicht jede Menge durch ein anderes dieser vier Elemente repräsentiert werden. Das heißt nichts anderes als dass es kein System verschiedener Repräsentanten von A_1, A_2, A_3, A_4, A_5 gibt.

(iii) Es gibt genau ein System verschiedener Repräsentanten, nämlich (D, C, A, B, E) . (Der letzte Eintrag muss ein E sein, dann muss der dritte Eintrag ein A sein, dann muss der zweite Eintrag ein C sein, dann muss der vierte Eintrag ein B sein und dann bleibt für den ersten Eintrag nur noch D übrig.)

Lösung von Aufgabe 107 Es gibt also 13 Stapel mit je vier Spielkarten. Wir betrachten diese Stapel als Mengen A_1, \dots, A_{13} . Uns interessieren aber nur die Werte der Karten, daher definieren wir für jedes $i \in \{1, \dots, 13\}$ die Mengen A'_i als die Menge aller Werte der Karten aus A_i . Die Behauptung können wir nun formulieren als: Es gibt ein (SvR) der Mengen A'_1, \dots, A'_{13} .

Da es nur vier Karten gleichen Wertes gibt, sind unter $4 \cdot k$ Karten, mit $k \in \{1, \dots, 13\}$, mindestens k verschiedene Werte vertreten. Das bedeutet nichts anderes, als $|\cup_{i \in I} A'_i| \geq |I|$ für alle $I \subseteq \{1, \dots, 13\}$. Mit dem Hochzeitssatz gibt es also mindestens ein (SvR) der Mengen A'_1, \dots, A'_{13} .

Lösung von Aufgabe 108 Die Bedingung (ii) besagt, dass wir die Namen der Personen aus einer Gruppe so in die Tabelle eintragen müssen, dass ein lateinisches Quadrat der Ordnung 5 entsteht. Bedingung (i) besagt, dass die Paare von Namen in jedem Eintrag der Tabelle verschieden sein müssen. Wir kürzen die Personen stets durch den Anfangsbuchstaben des Namens ab. Dann brauchen wir die Vereinigung von zwei orthogonalen lateinischen Quadraten der Ordnung 5, wobei das erste Einträge aus $\{A, B, C, D, E\}$ und das zweite Einträge aus $\{F, G, H, I, J\}$ besitzt.

Zu (a): Da 5 eine Primzahl ist, haben wir im Beweis von Theorem 7.18 ein Verfahren kennengelernt, wie wir orthogonale lateinische Quadrate der Ordnung 5 konstruieren können. Mit der Notation aus diesem Beweis und $p = 5$ erhalten wir, dass

$$L_1 : \begin{array}{ccccc} [2] & [3] & [4] & [0] & [1] \\ [3] & [4] & [0] & [1] & [2] \\ [4] & [0] & [1] & [2] & [3] \\ [0] & [1] & [2] & [3] & [4] \\ [1] & [2] & [3] & [4] & [0] \end{array}, L_2 : \begin{array}{ccccc} [3] & [4] & [0] & [1] & [2] \\ [0] & [1] & [2] & [3] & [4] \\ [2] & [3] & [4] & [0] & [1] \\ [4] & [0] & [1] & [2] & [3] \\ [1] & [2] & [3] & [4] & [0] \end{array}$$

$$\text{und } L_3 : \begin{array}{ccccc} [4] & [0] & [1] & [2] & [3] \\ [2] & [3] & [4] & [0] & [1] \\ [0] & [1] & [2] & [3] & [4] \\ [3] & [4] & [0] & [1] & [2] \\ [1] & [2] & [3] & [4] & [0] \end{array}$$

paarweise orthogonal sind. Weiter wissen wir, dass wir in jedem dieser lateinischen Quadrate die Einträge umbenennen können, ohne die Orthogonalität zu verändern. Betrachten wir die Vereinigung von L_1 und L_2 und ersetzen in L_1 die Elemente $[1], [2], [3], [4], [0]$ durch A, B, C, D, E (in dieser Reihenfolge) und in L_2 entsprechend, dann erhalten wir den Lernplan

	Ana 2	LinA 2	DM 2	Num 2	Rel 2
Montag	(B,H)	(C,I)	(D,J)	(E,F)	(A,G)
Dienstag	(C,J)	(D,F)	(E,G)	(A,H)	(B,I)
Mittwoch	(D,G)	(E,H)	(A,I)	(B,J)	(C,F)
Donnerstag	(E,I)	(A,J)	(B,F)	(C,G)	(D,H)
Freitag	(A,F)	(B,G)	(C,H)	(D,I)	(E,J)

der offensichtlich alle geforderten Eigenschaften erfüllt.

Zu (b): Nun brauchen wir drei paarweise orthogonale lateinische Quadrate der Ordnung 5. Glücklicherweise haben wir diese schon in (a) berechnet. Identifizieren wir in L_3 die Einträge $[1], [2], [3], [4], [0]$ mit K, L, M, N, O (in dieser Reihenfolge), liefert L_3 zusammen mit dem Lernplan aus (a) den Lernplan

	Ana 2	LinA 2	DM 2	Num 2	Rel 2
Montag	(B,H,N)	(C,I,O)	(D,J,K)	(E,F,L)	(A,G,M)
Dienstag	(C,J,L)	(D,F,M)	(E,G,N)	(A,H,O)	(B,I,K)
Mittwoch	(D,G,O)	(E,H,K)	(A,I,L)	(B,J,M)	(C,F,N)
Donnerstag	(E,I,M)	(A,J,N)	(B,F,O)	(C,G,K)	(D,H,L)
Freitag	(A,F,K)	(B,G,L)	(C,H,M)	(D,I,N)	(E,J,O)

Zu (c): Gäbe es einen Lernplan mit fünf Gruppen á fünf Personen, der (i)-(iii) erfüllt, so gäbe es fünf orthogonale lateinische Quadrate der Ordnung 5. Wir wissen allerdings, dass dies nicht der Fall ist (wieder Theorem 7.18), damit kann es einen solchen Lernplan nicht geben.

Lösung von Aufgabe 109 Orthogonale lateinische Quadrate der Ordnung 4 haben wir schon gesehen:

$$\begin{array}{l}
 D\heartsuit K\spadesuit A\diamond B\clubsuit \\
 B\clubsuit A\heartsuit K\clubsuit D\diamond \\
 K\diamond D\clubsuit B\heartsuit A\spadesuit \\
 A\clubsuit B\diamond D\spadesuit K\heartsuit
 \end{array}
 \text{ liefert }
 \begin{array}{l}
 \heartsuit \spadesuit \diamond \clubsuit \\
 \spadesuit \heartsuit \clubsuit \diamond \\
 \diamond \clubsuit \heartsuit \spadesuit \\
 \clubsuit \diamond \spadesuit \heartsuit
 \end{array}
 \text{ und }
 \begin{array}{l}
 D K A B \\
 B A K D \\
 K D B A \\
 A B D K
 \end{array}$$

Diese beiden lateinischen Quadrate sind orthogonal. Wir ersetzen $\heartsuit, \spadesuit, \diamond, \clubsuit$ auf irgendeine Art durch die Elemente 0, 1, 2, 3 und D, K, A, B auf irgendeine Art ebenfalls durch 0, 1, 2, 3. Dann sind die beiden lateinischen Quadrate, die wir erhalten, immer noch orthogonal. Wir entscheiden uns für

$$\begin{array}{l}
 0 \ 1 \ 2 \ 3 \\
 1 \ 0 \ 3 \ 2 \\
 2 \ 3 \ 0 \ 1 \\
 3 \ 2 \ 1 \ 0
 \end{array}
 L_1 : \quad \text{und} \quad \begin{array}{l}
 1 \ 2 \ 3 \ 0 \\
 0 \ 3 \ 2 \ 1 \\
 2 \ 1 \ 0 \ 3 \\
 3 \ 0 \ 1 \ 2
 \end{array}
 L_2 :$$

und erhalten

$$\begin{array}{l}
 (0, 1) \ (1, 2) \ (2, 3) \ (3, 0) \\
 (1, 0) \ (0, 3) \ (3, 2) \ (2, 1) \\
 (2, 2) \ (3, 1) \ (0, 0) \ (1, 3) \\
 (3, 3) \ (2, 0) \ (1, 1) \ (0, 2)
 \end{array}
 L_1 \cup L_2 :$$

Wir ersetzen nun wie vorgeschrieben (i, j) durch $4 \cdot i + j$ und erhalten

$$Q : \begin{array}{|c|c|c|c|} \hline 1 & 6 & 11 & 12 \\ \hline 4 & 3 & 14 & 9 \\ \hline 10 & 13 & 0 & 7 \\ \hline 15 & 8 & 5 & 2 \\ \hline \end{array}$$

Dies ist ein 4×4 Quadrat, in dem jede Zahl aus $\{0, \dots, 15\}$ genau einmal vorkommt. Die Summe der Einträge aus Zeile und die Summe der Einträge aus einer Spalte sind immer gleich 30.

Da L_1 und L_2 orthogonal sind, kommt in der Vereinigung jedes Tupel $(i, j) \in \{0, 1, 2, 3\}^2$ genau einmal vor. Da die Abbildung $\{0, 1, 2, 3\}^2 \longrightarrow \{0, \dots, 15\}$, mit

$(i, j) \mapsto 4 \cdot i + j$, offensichtlich bijektiv ist, kommt in Q jedes der Elemente aus $\{0, \dots, 15\}$ genau einmal vor. Weiter kommt in jeder Zeile und jeder Spalte von L_1 und L_2 jedes der Elemente aus $\{0, 1, 2, 3\}$ genau einmal vor. Damit ist jede Zeilen- und Spaltensumme gleich $4 \cdot (0 + 1 + 2 + 3) + (0 + 1 + 2 + 3) = 5 \cdot 6 = 30$.

1.8 Lösungen der Aufgaben aus Kapitel 8

Lösung von Aufgabe 110 Seien $A(x) = \sum_{n \geq 0} a_n \cdot x^n$, $B(x) = \sum_{n \geq 0} b_n \cdot x^n$, $C(x) = \sum_{n \geq 0} c_n \cdot x^n \in K[[x]]$, für einen Körper K . Dann ist

$$\begin{aligned} A(x) \cdot (B(x) + C(x)) &= \left(\sum_{n \geq 0} a_n \cdot x^n \right) \cdot \left(\sum_{n \geq 0} (b_n + c_n) \cdot x^n \right) \\ &= \sum_{n \geq 0} \left(\sum_{i=0}^n a_i \cdot (b_{n-i} + c_{n-i}) \right) \cdot x^n \\ &= \sum_{n \geq 0} \left(\sum_{i=0}^n (a_i \cdot b_{n-i} + a_i \cdot c_{n-i}) \right) \cdot x^n \\ &= \sum_{n \geq 0} \sum_{i=0}^n (a_i \cdot b_{n-i}) \cdot x^n + \sum_{n \geq 0} a_i \cdot c_{n-i} \cdot x^n \\ &= A(x) \cdot B(x) + A(x) \cdot C(x) \end{aligned}$$

Damit gilt das Distributivgesetz auf $K[[x]]$.

Lösung von Aufgabe 111 Wir führen eine Induktion über k .

Induktionsanfang: Für $k = 2$ ist per Definition $\left(\sum_{n \geq 0} a_n^{(1)} x^n \right) \cdot \left(\sum_{n \geq 0} a_n^{(2)} x^n \right) = \sum_{n \geq 0} \left(\sum_{i=0}^n a_i^{(1)} \cdot a_{n-i}^{(2)} \right) x^n$. Da wir $r_1 + r_2 = n$, mit $r, s \in \{0, \dots, n\}$, haben genau dann wenn $r = i$ und $s = n - i$ für ein $i \in \{0, \dots, n\}$ ist, folgt die gewünschte Gleichung

$$\left(\sum_{n \geq 0} a_n^{(1)} x^n \right) \cdot \left(\sum_{n \geq 0} a_n^{(2)} x^n \right) = \sum_{n \geq 0} \left(\sum_{i=0}^n a_i^{(1)} \cdot a_{n-i}^{(2)} \right) x^n = \sum_{n \geq 0} \left(\sum_{r_1+r_2=n} a_{r_1}^{(1)} \cdot a_{r_2}^{(2)} \right) x^n.$$

Induktionsvoraussetzung: Für beliebiges aber festes $k \geq 2$ gelte:

Sind $\left(\sum_{n \geq 0} a_n^{(1)} x^n \right), \dots, \left(\sum_{n \geq 0} a_n^{(k)} x^n \right) \in K[[x]]$, so ist

$$\left(\sum_{n \geq 0} a_n^{(1)} x^n \right) \cdot \dots \cdot \left(\sum_{n \geq 0} a_n^{(k)} x^n \right) = \sum_{n \geq 0} \left(\sum_{r_1+\dots+r_k=n} a_{r_1}^{(1)} \cdot \dots \cdot a_{r_k}^{(k)} \right) x^n \quad (1.13)$$

Induktionsschritt: Sei k aus der Induktionsvoraussetzung. Wir müssen zeigen, dass (1.13) auch gilt, wenn wir k durch $k + 1$ ersetzen. Es ist

$$\begin{aligned}
& \left(\sum_{n \geq 0} a_n^{(1)} x^n \right) \cdot \dots \cdot \left(\sum_{n \geq 0} a_n^{(k+1)} x^n \right) \\
&= \left(\left(\sum_{n \geq 0} a_n^{(1)} x^n \right) \cdot \dots \cdot \left(\sum_{n \geq 0} a_n^{(k)} x^n \right) \right) \cdot \left(\sum_{n \geq 0} a_n^{(k+1)} x^n \right) \\
&\stackrel{IV}{=} \left(\sum_{n \geq 0} \left(\sum_{r_1 + \dots + r_k = n} a_{r_1}^{(1)} \cdot \dots \cdot a_{r_k}^{(k)} \right) x^n \right) \cdot \left(\sum_{n \geq 0} a_n^{(k+1)} x^n \right)
\end{aligned}$$

Für jedes $n \in \mathbb{N}_0$ setzen wir $b_n = \sum_{r_1 + \dots + r_k = n} a_{r_1}^{(1)} \cdot \dots \cdot a_{r_k}^{(k)}$. Damit ist dann

$$\begin{aligned}
\left(\sum_{n \geq 0} a_n^{(1)} x^n \right) \cdot \dots \cdot \left(\sum_{n \geq 0} a_n^{(k+1)} x^n \right) &= \left(\sum_{n \geq 0} b_n x^n \right) \cdot \left(\sum_{n \geq 0} a_n^{(k+1)} x^n \right) \\
&= \sum_{n \geq 0} \left(\sum_{i=0}^n b_i \cdot a_{n-i}^{(k+1)} \right) x^n.
\end{aligned}$$

Der n -te Koeffizient von $\left(\sum_{n \geq 0} a_n^{(1)} x^n \right) \cdot \dots \cdot \left(\sum_{n \geq 0} a_n^{(k+1)} x^n \right)$ ist damit gleich

$$\begin{aligned}
\sum_{i=0}^n b_i \cdot a_{n-i}^{(k+1)} &= \sum_{r+r_{k+1}=n} \left(\sum_{r_1 + \dots + r_k = r} a_{r_1}^{(1)} \cdot \dots \cdot a_{r_k}^{(k)} \right) \cdot a_{r_{k+1}}^{(k+1)} \\
&= \sum_{r_1 + \dots + r_{k+1} = n} a_{r_1}^{(1)} \cdot \dots \cdot a_{r_{k+1}}^{(k+1)}.
\end{aligned}$$

Das war zu zeigen.

Lösung von Aufgabe 112 Zu (a): Es ist

$$\begin{aligned}
& \left(\sum_{n \geq 4} b_{n+1} \cdot x^{n-3} \right) \cdot \left(\sum_{n \geq 0} 2^n \cdot c_n \cdot x^n \right) = \left(\sum_{n \geq 1} b_{n+4} \cdot x^n \right) \cdot \left(\sum_{n \geq 0} 2^n \cdot c_n \cdot x^n \right) \\
&= \sum_{n \geq 0} \left(\sum_{i=1}^n b_{i+4} \cdot 2^{n-i} \cdot c_{n-i} \right) x^n \\
&= \sum_{n \geq 1} \left(\sum_{i=1}^n b_{i+4} \cdot 2^{n-i} \cdot c_{n-i} \right) x^n.
\end{aligned}$$

Damit haben wir das Produkt als eine Potenzreihe der Form $\sum_{n \geq k} a_n x^n$ geschrieben (mit $k = 1$ und $a_n = \sum_{i=1}^n b_{i+4} \cdot 2^{n-i} \cdot c_{n-i}$ für alle $n \in \mathbb{N}_0$).

Zu (b): Sei nun $b_n = b$, für festes $b \in K$ und für alle $n \in \mathbb{N}_0$. Dann ist

$$\begin{aligned}
\left(\sum_{n \geq 0} b_n x^n\right)^2 &= \left(\sum_{n \geq 0} b_n x^n\right) \cdot \left(\sum_{n \geq 0} b_n x^n\right) = \sum_{n \geq 0} \left(\sum_{i=0}^n b_i \cdot b_{n-i}\right) x^n \\
&= \sum_{n \geq 0} \left(\sum_{i=0}^n b^2\right) x^n = \sum_{n \geq 0} (n+1) \cdot b^2 \cdot x^n.
\end{aligned}$$

Lösung von Aufgabe 113 Für beide Aufgabenteile genügt es die Formel aus Korollar 8.18 anzuwenden.

Zu (a): Aus $\sum_{n \geq 0} x^{k \cdot n} = \sum_{n \geq 0} \binom{1+n-1}{n} \cdot x^{k \cdot n} = \frac{1}{1-x^k}$ folgt unmittelbar, dass das multiplikative Inverse von $\sum_{n \geq 0} x^{k \cdot n}$ gleich $1 - x^k$ ist.

Zu (b): Aus $\sum_{n \geq 0} (-1)^n x^{k \cdot n} = \sum_{n \geq 0} \binom{1+n-1}{n} \cdot (-1)^n \cdot x^{k \cdot n} = \frac{1}{1-(-1) \cdot x^k} = \frac{1}{1+x^k}$ folgt unmittelbar, dass das multiplikative Inverse von $\sum_{n \geq 0} (-1)^n x^{k \cdot n}$ gleich $1 + x^k$ ist.

Lösung von Aufgabe 114 Ein multiplikatives Inverses von $\sum_{n \geq 0} a_n x^n$ ist eine formale Potenzreihe $\sum_{n \geq 0} b_n x^n$ mit $(\sum_{n \geq 0} a_n x^n) \cdot (\sum_{n \geq 0} b_n x^n) = 1$.

Zu (a): Da der 0-te Koeffizient von $f(x)$ gleich $[2] \neq [0]$ ist, existiert ein multiplikatives Inverses $\sum_{n \geq 0} b_n x^n \in \mathbb{Z}/7\mathbb{Z}[[x]]$ von $f(x)$. Es gilt

$$[1] = \left(\sum_{n \geq 0} [2 \cdot (n+1)] x^n\right) \cdot \left(\sum_{n \geq 0} b_n x^n\right) = \sum_{n \geq 0} \left(\sum_{i=0}^n [2(i+1)] \cdot b_{n-i}\right) x^n$$

Es gilt also $[1] = [2] \cdot b_0$ und somit $b_0 = [4]$. Nun folgt sukzessive:

- $[0] = [2] \cdot b_1 + [4] \cdot b_0 \implies b_1 = [6]$
- $[0] = [2] \cdot b_2 + [4] \cdot b_1 + [6] \cdot b_0 \implies b_2 = [4]$
- $[0] = [2] \cdot b_3 + [4] \cdot b_2 + [6] \cdot b_1 + [1] \cdot b_0 \implies b_3 = [0]$
- $[0] = [2] \cdot b_4 + [4] \cdot b_3 + [6] \cdot b_2 + [1] \cdot b_1 + [3] \cdot b_0 \implies b_4 = [0]$

Zu (b): Aus $a_0 = 1 \neq 0$ folgt sofort, dass ein multiplikatives Inverses $\sum_{n \geq 0} b_n x^n \in \mathbb{C}[[x]]$ von $f(x)$ existiert. Wir nutzen $f(x) = 1 + 0 \cdot x + 1 \cdot x^2 + 1 \cdot 3 + 0 \cdot x^4 + 1 \cdot x^5 + \dots$ und erhalten wie in (a):

- $1 = 1 \cdot b_0 \implies b_0 = 1$
- $0 = 1 \cdot b_1 + 0 \cdot b_0 \implies b_1 = 0$
- $0 = 1 \cdot b_2 + 0 \cdot b_1 + 1 \cdot b_0 \implies b_2 = -\frac{1}{2}$
- $0 = 1 \cdot b_3 + 0 \cdot b_2 + 1 \cdot b_1 + 1 \cdot b_0 \implies b_3 = -\frac{1}{2}$
- $0 = 1 \cdot b_4 + 0 \cdot b_3 + 1 \cdot b_2 + 1 \cdot b_1 + 0 \cdot b_0 \implies b_4 = \frac{1}{2}$

Lösung von Aufgabe 115 Angenommen es gibt eine formale Potenzreihe $f(x) \in \mathbb{Z}/p\mathbb{Z}[[x]]$, mit $D(f(x)) = f(x)$. Wir schreiben $f(x) = \sum_{n \geq 0} a_n x^n$. Dann gilt

$$\sum_{n \geq 0} a_n x^n = D \left(\sum_{n \geq 0} a_n x^n \right) = \sum_{n \geq 0} \underbrace{(n+1)a_{n+1}}_{=a_{n+1} + \dots + a_{n+1} \text{ (n+1)-mal}} x^n = \sum_{n \geq 0} [n+1]a_{n+1} x^n.$$

Sei nun $k \in \mathbb{N}_0$ beliebig. Dann ist $a_{kp-1} = [kp]a_{kp} = [0]$. Damit ist aber auch $a_{kp-2} = [kp-1] \cdot a_{kp-1} = [0]$ und induktiv folgt, dass $a_n = [0]$ für alle $n \leq kp-1$. Da dies für beliebiges k gilt, ist $a_n = [0]$ für alle $n \in \mathbb{N}_0$ und somit ist $f(x) = 0$. Insbesondere gibt es kein $f(x) \in \mathbb{Z}/p\mathbb{Z}[[x]] \setminus \{[0]\}$, mit $D(f(x)) = f(x)$.

Lösung von Aufgabe 116 Wir benutzen im folgenden das „Vokabelheft“ von Seite 191. Damit und mit der Definition der Multiplikation erhalten wir

$$\begin{aligned} \sum_{n \geq 0} \left(\sum_{i=0}^n \binom{i+k}{i} \cdot \binom{n-i+l}{n-i} \right) x^n &= \sum_{n \geq 0} \binom{n+k}{n} x^n + \sum_{n \geq 0} \binom{n+l}{n} x^n \\ &= \frac{1}{(1-x)^{k+1}} \cdot \frac{1}{(1-x)^{l+1}} = \frac{1}{(1-x)^{k+l+2}} \\ &= \sum_{n \geq 0} \binom{n+k+l+1}{n} x^n \end{aligned}$$

Koeffizientenvergleich liefert sofort die gewünschte Gleichung

$$\sum_{i=0}^n \binom{i+k}{i} \cdot \binom{n-i+l}{n-i} = \binom{n+k+l+1}{n} \quad \forall k, l, n \in \mathbb{N}_0.$$

Lösung von Aufgabe 117 Es ist

$$\frac{A}{1-ax} + \frac{B}{1-bx} = \frac{A(1-bx) + B(1-ax)}{(1-ax)(1-bx)} = \frac{-(Ab+Ba)x + (A+B)}{(1-ax)(1-bx)}.$$

Wir müssen $A, B \in K$ also so wählen, dass $1 = -(Ab+Ba)x + (A+B)$ gilt. Koeffizientenvergleich liefert uns, dass das genau dann der Fall ist, wenn

$$-(Ab+Ba) = 0 \quad \text{und} \quad A+B = 1$$

gilt. Damit ist $A = 1 - B$ und $(1-B)b + Ba = 0$. Also gilt $B = \frac{b}{b-a}$ und $A = 1 - \frac{b}{b-a} = \frac{a}{a-b}$. Diese Werte sind auch tatsächlich definiert, da $a \neq b$ gilt.

Kommen wir nun zur Berechnung von A' und B' . Genau wie eben erhalten wir, dass A' und B' genau die Elemente aus K sind, die die Bedingungen

$$A' + B' = 0 \quad \text{und} \quad -(A'b + B'a) = 1$$

erfüllen. Damit folgt $B' = \frac{1}{b-a}$ und $A' = \frac{1}{a-b}$. Wieder brauchen wir hierfür die Bedingung $a \neq b$.

Lösung von Aufgabe 118 Wir studieren in dieser Aufgabe das Polynom $f(x) = -x^4 + 2x^3 - 2x + 1$ und die formale Potenzreihe $\frac{1}{f(x)} \in \mathbb{C}[[x]]$.

Zu (a): Es ist $f(1) = 0$ und $f(-1) = 0$. Damit ist $f(x)$ durch $(x - 1)$ und durch $(x + 1)$ – also durch $(x - 1) \cdot (x + 1) = x^2 - 1$ – teilbar. Wir benutzen Polynomdivision und erhalten

$$f \div (x^2 - 1) = -(x^2 - 2x + 1) = -(x - 1)^2.$$

Es folgt sofort

$$f(x) = -(x - 1)^2 \cdot (x^2 - 1) = -(x - 1)^3 \cdot (x + 1) = (1 - x)^3 \cdot (1 + x).$$

Insbesondere ist $a = 1$, $b = -1$, $r_a = 3$ und $r_b = 1$.

Zu (b): Da $1 \neq -1$, existieren Polynome $A(x)$ und $B(x)$, die die Gleichung

$$\frac{1}{(1 - x)^3 \cdot (1 + x)} = \frac{A(x)}{(1 - x)^3} + \frac{B(x)}{(1 + x)} \quad (1.14)$$

erfüllen. Weiter wissen wir, dass $\text{grad}(A) < 3$ und $\text{grad}(B) < 1$ ist. Damit existieren $a_2, a_1, a_0, b \in \mathbb{C}$, mit

$$A(x) = a_2 x^2 + a_1 x + a_0 \quad \text{und} \quad B(x) = b.$$

Es folgt, dass (1.14) äquivalent ist zu

$$\begin{aligned} \frac{1}{(1 - x)^3 \cdot (1 + x)} &= \frac{A(x) \cdot (1 + x) + B(x) \cdot (1 - x)^3}{(1 - x)^3 \cdot (1 + x)} \\ \iff 1 &= A(x) \cdot (1 + x) + B(x) \cdot (1 - x)^3 \\ \iff 1 &= (a_2 - b)x^3 + (a_1 + a_2 + 3b)x^2 + (a_1 + a_0 - 3b)x + (a_0 + b) \\ \iff a_2 - b &= 0, \quad a_1 + a_2 + 3b = 0, \quad a_1 + a_0 - 3b = 0, \quad \text{und} \quad a_0 + b = 1 \\ \iff a_2 &= b, \quad a_1 + 4a_2 = 0, \quad a_1 + a_0 - 3a_2 = 0, \quad \text{und} \quad a_0 + a_2 = 1 \\ \iff a_2 &= b, \quad a_1 = -4a_2, \quad a_0 - 7a_2 = 0, \quad \text{und} \quad a_0 + a_2 = 1 \\ \iff a_2 &= b, \quad a_1 = -4a_2, \quad a_0 = 7a_2, \quad \text{und} \quad 8a_2 = 1 \\ \iff b &= \frac{1}{8}, \quad a_1 = -\frac{4}{8} = -\frac{1}{2}, \quad a_0 = \frac{7}{8}, \quad \text{und} \quad a_2 = \frac{1}{8} \\ \iff A(x) &= \frac{1}{8}x^2 - \frac{1}{2}x + \frac{7}{8} \quad \text{und} \quad B(x) = \frac{1}{8}. \end{aligned}$$

Zu (c): Es ist

$$\begin{aligned}
\frac{1}{f(x)} &\stackrel{\text{(a)}}{=} \frac{1}{(1-x)^3 \cdot (1+x)} \stackrel{\text{(b)}}{=} \frac{\frac{1}{8}x^2 - \frac{1}{2}x + \frac{7}{8}}{(1-x)^3} + \frac{\frac{1}{8}}{(1+x)} \\
&= \left(\frac{1}{8}x^2 - \frac{1}{2}x + \frac{7}{8}\right) \cdot \sum_{n \geq 0} \binom{n+2}{n} x^n + \frac{1}{8} \cdot \sum_{n \geq 0} (-1)^n x^n \\
&= \frac{1}{8} \cdot \left(\sum_{n \geq 0} \binom{n+2}{n} x^{n+2} - 4 \cdot \sum_{n \geq 0} \binom{n+2}{n} x^{n+1} \right. \\
&\quad \left. + 7 \cdot \sum_{n \geq 0} \binom{n+2}{n} x^n + 8 \cdot \sum_{n \geq 0} (-1)^n x^n \right) \\
&= \frac{1}{8} \cdot \left(1 + 2x + \sum_{n \geq 2} \left(\binom{n}{n-2} - 4 \binom{n+1}{n-1} + 7 \binom{n+2}{n} + (-1)^n \right) x^n \right) \tag{1.15}
\end{aligned}$$

Im letzten Schritt haben wir nur die ersten beiden Koeffizienten separat berechnet und danach die Indizes so verschoben, dass wir alles zu einer formalen Potenzreihe zusammenfassen konnten. Wir schreiben die Koeffizienten der letzten Zeile nochmal auf ohne Binomialkoeffizienten zu benutzen:

$$\underbrace{\binom{n}{n-2}}_{=\frac{n(n-1)}{2}} - 4 \underbrace{\binom{n+1}{n-1}}_{=\frac{(n+1)n}{2}} + 7 \underbrace{\binom{n+2}{n}}_{=\frac{(n+2)(n+1)}{2}} + (-1)^n = 2n^2 + 8n + 7 + (-1)^n.$$

Setzen wir dies in (1.15) ein, erhalten wir

$$\begin{aligned}
\frac{1}{f(x)} &= \frac{1}{8} \cdot \left(1 + 2x + \sum_{n \geq 2} (2n^2 + 8n + 7 + (-1)^n) x^n \right) \\
&= \sum_{n \geq 0} \frac{1}{8} (2n^2 + 8n + 7 + (-1)^n) x^n.
\end{aligned}$$

Zu (d): Wir berechnen $\frac{1}{f(x)}$ nochmal auf eine andere Art. Der Anfang ist genau wie in Teil (b), allerdings benutzen wir dann direkt die Definition der Multiplikation auf $\mathbb{C}[[x]]$:

$$\begin{aligned}
\frac{1}{f(x)} &= \frac{1}{(1-x)^3} \cdot \frac{1}{(1+x)} = \left(\sum_{n \geq 0} \binom{n+2}{n} x^n \right) \cdot \left(\sum_{n \geq 0} (-1)^n x^n \right) \\
&= \sum_{n \geq 0} \left(\sum_{i=0}^n (-1)^{n-i} \cdot \binom{i+2}{i} \right) x^n.
\end{aligned}$$

Vergleichen wir dies mit unserem Ergebnis aus Teil (c), so folgt

$$\sum_{i=0}^n (-1)^{n-i} \cdot \binom{i+2}{i} = \frac{1}{8} (2n^2 + 8n + 7 + (-1)^n) \quad \forall n \in \mathbb{N}_0.$$

Lösung von Aufgabe 119 Seien c, d und a_n wie in der Aufgabenstellung. Wir betrachten die erzeugende Funktion $A(x)$ von $(a_n)_{n \in \mathbb{N}_0}$ und erhalten

$$\begin{aligned} A(x) &= \sum_{n \geq 0} a_n x^n \stackrel{a_0=0}{=} \sum_{n \geq 1} a_n x^n = \sum_{n \geq 1} (c \cdot a_{n-1} + d) x^n \\ &= \sum_{n \geq 1} c \cdot a_{n-1} x^n + \sum_{n \geq 1} d x^n = c \cdot \sum_{n \geq 1} a_{n-1} x^n + d \cdot \sum_{n \geq 1} x^n \\ &= c \cdot \sum_{n \geq 0} a_n x^{n+1} + d \cdot x \cdot \sum_{n \geq 0} x^n = c \cdot x \cdot A(x) + d \cdot x \cdot \frac{1}{1-x}. \end{aligned}$$

Umstellen dieser Gleichung liefert

$$(1 - c \cdot x) \cdot A(x) = \frac{d \cdot x}{1-x} \implies A(x) = d \cdot x \cdot \frac{1}{(1-x) \cdot (1-c \cdot x)} \quad (1.16)$$

Falls $c = 1$ ist, so erhalten wir

$$A(x) = d \cdot x \cdot \frac{1}{(1-x)^2} = d \cdot x \cdot \sum_{n \geq 0} \binom{n+1}{n} x^n = \sum_{n \geq 0} d \cdot (n+1) x^{n+1} = \sum_{n \geq 1} d n x^n = \sum_{n \geq 0} d n x^n.$$

Durch Vergleichen der Koeffizienten erhalten wir $a_n = dn$ für alle $n \in \mathbb{N}_0$, falls $c = 1$.

Falls $c \neq 1$, so können wir Aufgabe 117 benutzen und erhalten aus (1.16)

$$\begin{aligned} A(x) &= d \cdot x \cdot \left(\frac{1}{1-c} \cdot \frac{1}{1-x} + \frac{c}{c-1} \cdot \frac{1}{1-c \cdot x} \right) \\ &= d \cdot x \cdot \left(\frac{1}{1-c} \cdot \sum_{n \geq 0} x^n + \frac{c}{c-1} \cdot \sum_{n \geq 0} c^n x^n \right) \\ &= d \cdot x \cdot \sum_{n \geq 0} \left(\frac{1}{1-c} + \frac{c^{n+1}}{c-1} \right) x^n = \sum_{n \geq 0} d \cdot \frac{1-c^{n+1}}{1-c} x^{n+1} \\ &= \sum_{n \geq 1} d \cdot \frac{1-c^n}{1-c} x^n = \sum_{n \geq 0} d \cdot \frac{1-c^n}{1-c} x^n. \end{aligned}$$

Das letzte Gleichheitszeichen folgt aus der Beobachtung, dass $0 = d \cdot \frac{1-c^0}{1-c}$ gilt. Wieder vergleiche wir die Koeffizienten und erhalten $a_n = d \cdot \frac{1-c^n}{1-c}$ für alle $n \in \mathbb{N}_0$, falls $c \neq 1$.

Lösung von Aufgabe 120 Wir betrachten die erzeugende Funktion $A(x)$ von der rekursiv definierten Folge a_0, a_1, \dots . Diese wollen wir zunächst als Quotient von

zwei Polynomen schreiben. Dazu benutzen wir nur die Definition der Rekursion, Indexshift und unsere Formelsammlung von Seite 191.

$$\begin{aligned}
 A(x) &= \sum_{n \geq 0} a_n x^n = a_0 + a_1 x + \sum_{n \geq 2} a_n x^n = x + \sum_{n \geq 2} (2a_{n-1} - a_{n-2} + 1)x^n \\
 &= x + \sum_{n \geq 2} 2a_{n-1} x^n - \sum_{n \geq 2} a_{n-2} x^n + \sum_{n \geq 2} x^n \\
 &= 2 \cdot \sum_{n \geq 1} a_n x^{n+1} - \sum_{n \geq 0} a_n x^{n+2} + \underbrace{\sum_{n \geq 1} x^n}_{=x \cdot \sum_{n \geq 0} x^n}
 \end{aligned}$$

Im letzten Schritt haben wir zweimal den Index verschoben und $x + \sum_{n \geq 2} x^n$ zu $\sum_{n \geq 1} x^n$ zusammengefasst. Das war bis hierhin eigentlich das schwierigste der Aufgabe. Wir rechnen nun weiter und erhalten

$$\begin{aligned}
 A(x) &= 2 \cdot x \cdot \underbrace{\sum_{n \geq 1} a_n x^n}_{\stackrel{a_0=0}{=} A(x)} - x^2 \cdot \underbrace{\sum_{n \geq 0} a_n x^n}_{=A(x)} + x \cdot \frac{1}{1-x} \\
 &= (-x^2 + 2x) \cdot A(x) + x \cdot \frac{1}{1-x}.
 \end{aligned}$$

Umstellen der Gleichung liefert

$$\underbrace{(x^2 - 2x + 1)}_{=(1-x)^2} \cdot A(x) = x \cdot \frac{1}{1-x} \implies A(x) = x \cdot \frac{1}{(1-x)^3}$$

Dies schreiben wir mit unserer Formelsammlung wieder als formale Potenzreihe:

$$\begin{aligned}
 A(x) &= x \cdot \sum_{n \geq 0} \binom{n+2}{n} x^n = \sum_{n \geq 0} \underbrace{\binom{n+2}{n}}_{=\frac{(n+2)(n+1)}{2}} x^{n+1} = \sum_{n \geq 1} \frac{(n+1) \cdot n}{2} x^n \\
 &\stackrel{a_0=0}{=} \sum_{n \geq 0} \frac{(n+1) \cdot n}{2} x^n
 \end{aligned}$$

Vergleichen der Koeffizienten liefert nun endlich $a_n = \frac{(n+1) \cdot n}{2}$ für alle $n \in \mathbb{N}_0$.

Lösung von Aufgabe 121 Für die erzeugende Funktion von s_0, s_1, \dots gilt

$$S(x) = \sum_{n \geq 0} s_n x^n = \sum_{n \geq 0} \left(\sum_{i=0}^n i^3 \right) x^n = \left(\sum_{n \geq 0} n^3 x^n \right) \cdot \frac{1}{1-x}. \quad (1.17)$$

Wir wollen also zunächst $\sum_{n \geq 0} n^3 x^n$ genauer studieren. Dazu berechnen wir

$$\begin{aligned} \sum_{n \geq 0} n^3 x^n &= 0^3 + \sum_{n \geq 1} n^3 x^n = \sum_{n \geq 0} (n+1)^3 x^{n+1} = x \cdot \sum_{n \geq 0} (n+1)^3 x^n \\ &= x \cdot D \left(\sum_{n \geq 0} n^2 x^n \right) = x \cdot \frac{x^2 + 4x + 1}{(1-x)^4} = \frac{x^3 + 4x^2 + x}{(1-x)^4}. \end{aligned}$$

Setzen wir dies in (1.17) ein, erhalten wir

$$\begin{aligned} S(x) &= \frac{x^3 + 4x^2 + x}{(1-x)^5} = (x^3 + 4x^2 + x) \cdot \sum_{n \geq 0} \binom{n+4}{n} x^n \\ &= x^3 \cdot \sum_{n \geq 0} \binom{n+4}{n} x^n + 4x^2 \cdot \sum_{n \geq 0} \binom{n+4}{n} x^n + x \cdot \sum_{n \geq 0} \binom{n+4}{n} x^n \\ &= \sum_{n \geq 0} \binom{n+4}{n} x^{n+3} + \sum_{n \geq 0} 4 \binom{n+4}{n} x^{n+2} + \sum_{n \geq 0} \binom{n+4}{n} x^{n+1}. \end{aligned}$$

Wir berechnen die ersten drei Koeffizienten dieser formalen Potenzreihe direkt und verschieben dann die Indizes passend. Damit ergibt sich

$$\begin{aligned} S(x) &= x + 9x^2 + \sum_{n \geq 3} \binom{n+1}{n-3} x^n + \sum_{n \geq 3} 4 \binom{n+2}{n-2} x^n + \sum_{n \geq 3} \binom{n+3}{n-1} x^n \\ &= x + 9x^2 + \sum_{n \geq 3} \left(\binom{n+1}{n-3} + 4 \binom{n+2}{n-2} + \binom{n+3}{n-1} \right) x^n. \end{aligned}$$

Koeffizientenvergleich gibt uns die Formel $s_n = \binom{n+1}{n-3} + 4 \binom{n+2}{n-2} + \binom{n+3}{n-1}$ für alle $n \geq 3$. Diese Formel wollen wir noch etwas handlicher aufschreiben. Sei also $n \geq 3$ beliebig. Dann gilt

$$\begin{aligned} s_n &= \binom{n+1}{n-3} + 4 \binom{n+2}{n-2} + \binom{n+3}{n-1} \\ &= \frac{(n+1)n(n-1)(n-2)}{4!} + 4 \cdot \frac{(n+2)(n+1)n(n-1)}{4!} + \frac{(n+3)(n+2)(n+1)n}{4!} \\ &= \frac{(n+1)n}{4!} \cdot ((n-1)(n-2) + 4(n+2)(n-1) + (n+3)(n+2)) \\ &= \frac{(n+1)n}{4!} \cdot (6n^2 + 6n) = \frac{(n+1)n}{4!} \cdot 3! \cdot (n+1) \cdot n = \frac{(n+1)^2 n^2}{4}. \end{aligned}$$

Es ist allerdings auch $s_0 = 0 = \frac{(0+1)^2 0^2}{4}$, $s_1 = 1 = \frac{(1+1)^2 1^2}{4}$ und $s_2 = 8 = \frac{(2+1)^2 2^2}{4}$. Damit gilt für alle $n \in \mathbb{N}_0$ die Formel

$$s_n = \sum_{i=0}^n i^3 = \frac{(n+1)^2 n^2}{4}.$$

Lösung von Aufgabe 122 Die binomische Formel gilt natürlich auch im Ring $\mathbb{C}[[x]]$. Es ist also insbesondere

$$(x \cdot f(x) + 1)^2 = (x \cdot f(x))^2 + 2 \cdot x \cdot f(x) + 1 \quad (1.18)$$

für jedes $f(x) \in \mathbb{C}[[x]]$. Streng genommen dürfen wir nicht „durch x teilen“, da x keine Einheit in $\mathbb{C}[[x]]$ ist. Wir dürfen x jedoch aus einer Gleichung *kürzen*, da $\mathbb{C}[[x]]$ nullteilerfrei ist. Sind $g(x), h(x) \in \mathbb{C}[[x]]$ beliebig, dann ist

$$x \cdot g(x) = x \cdot h(x) \implies \underbrace{x}_{\neq 0} \cdot (g(x) - h(x)) = 0 \implies g(x) - h(x) = 0 \implies g(x) = h(x).$$

Das werden wir im folgenden frei benutzen. Sei nun $f(x) \in \mathbb{C}[[x]]$. Dann gilt

$$\begin{aligned} x \cdot f(x)^2 + 2 \cdot f(x) + 6 &= 0 \\ \iff (x \cdot f(x))^2 + 2 \cdot x \cdot f(x) + 6 \cdot x &= 0 \\ \stackrel{(1.18)}{\iff} (x \cdot f(x) + 1)^2 + 6 \cdot x - 1 &= 0 \\ \iff (x \cdot f(x) + 1)^2 = 1 - 6 \cdot x. \end{aligned}$$

Diese letzte Gleichung gilt also genau dann, wenn $x \cdot f(x) + 1$ ein Wurzel von $1 - 6 \cdot x$ ist mit 0-tem Koeffizienten gleich 1. Davon gibt es nur eine und diese wurde in (8.6) berechnet (wir müssen lediglich x durch $6 \cdot x$ ersetzen). Es ist also

$$\begin{aligned} x \cdot f(x)^2 + 2 \cdot f(x) + 6 &= 0 \\ \iff x \cdot f(x) + 1 &= 1 - \sum_{n \geq 1} \frac{(2 \cdot (n-1))!}{2^{2n-1} \cdot (n-1)! \cdot n!} \cdot 6^n \cdot x^n \\ \iff f(x) &= - \sum_{n \geq 1} \frac{(2 \cdot (n-1))!}{2^{2n-1} \cdot (n-1)! \cdot n!} \cdot 2^n \cdot 3^n \cdot x^{n-1} \\ \iff f(x) &= - \sum_{n \geq 0} \frac{(2 \cdot n)!}{2^n \cdot n! \cdot (n+1)!} \cdot 3^{n+1} \cdot x^n = - \sum_{n \geq 0} \frac{3^{n+1}}{2^n \cdot (n+1)} \cdot \binom{2n}{n} \cdot x^n \end{aligned}$$

Lösung von Aufgabe 123 Sei R ein nullteilerfreier Ring und $a \in R$. Falls es kein Element $x \in R$ gibt, mit $x^2 = a$ sind wir fertig. Sei also $x \in R$, mit $x^2 = a$ gegeben. Sei nun $y \in R$ ein Element, das ebenfalls die Gleichung $y^2 = a$ erfüllt. Dann folgt

$$x^2 = y^2 \implies 0 = x^2 - y^2 = (x - y) \cdot (x + y).$$

Da R nullteilerfrei ist, folgt daraus, dass $x - y = 0$ oder $x + y = 0$ gilt. Das bedeutet aber, dass $y = -x$ oder $y = x$ gilt. Damit sind $x, -x \in R$ die einzigen Elemente, die quadriert a ergeben. Insbesondere gibt es maximal zwei solcher Elemente.

Lösung von Aufgabe 124 Sei $n \in \mathbb{N}_0$ beliebig. Die Menge $\{n-i \mid i \in \{0, \dots, n-1\}\}$ ist natürlich nichts anderes als die Menge $\{1, \dots, n\}$. Damit ist

$$\left(-\frac{3}{2}\right)^{[n]} = \prod_{i=0}^{n-1} \left(-\frac{3}{2} + n - i\right) = \prod_{i=1}^n \left(-\frac{3}{2} + i\right) = \prod_{i=0}^{n-1} \left(-\frac{3}{2} + (i+1)\right) = \prod_{i=0}^{n-1} \left(-\frac{1}{2} + i\right).$$

Ziehen wir aus jedem der Faktoren auf der rechten Seite den Faktor (-1) heraus, erhalten wir

$$\left(-\frac{3}{2}\right)^{[n]} = (-1)^n \cdot \prod_{i=0}^{n-1} \left(\frac{1}{2} - i\right) = (-1)^n \cdot \left(\frac{1}{2}\right)^{[n]}.$$

Es folgt nun unmittelbar

$$\binom{-\frac{3}{2}}{n} = \frac{\left(-\frac{3}{2}\right)^{[n]}}{n!} = \frac{(-1)^n \cdot \left(\frac{1}{2}\right)^{[n]}}{n!} = (-1)^n \cdot \binom{\frac{1}{2}}{n},$$

was zu zeigen war.

Lösung von Aufgabe 125 Seien wie gewünscht $\alpha, \beta \in \mathbb{C}$ und $n \in \mathbb{N}_0$ beliebig.

Zu (a): Wir rechnen die Gleichheit einfach aus:

$$\begin{aligned} \binom{\alpha-1}{n+1} + \binom{\alpha-1}{n} &= \frac{(\alpha-1)^{[n+1]}}{(n+1)!} + \frac{(\alpha-1)^{[n]}}{n!} \\ &= \frac{\prod_{i=0}^n (\alpha-1-i)}{(n+1)!} + \frac{\prod_{i=0}^{n-1} (\alpha-1-i)}{n!} \\ &= (\alpha-1-n) \cdot \frac{\prod_{i=0}^{n-1} (\alpha-1-i)}{(n+1)!} + (n+1) \cdot \frac{\prod_{i=0}^{n-1} (\alpha-1-i)}{(n+1)!} \\ &= \frac{\prod_{i=0}^{n-1} (\alpha-1-i) \cdot (\alpha-1-n+n+1)}{(n+1)!} = \frac{\alpha \cdot \prod_{i=0}^{n-1} (\alpha-1-i)}{(n+1)!} \\ &= \frac{\prod_{i=0}^n (\alpha-i)}{(n+1)!} = \frac{\alpha^{[n]}}{n+1} = \binom{\alpha}{n+1} \end{aligned}$$

Das war zu zeigen.

Zu (b): *Induktionsanfang:* $\boxed{n=0}$ Aus $1 = \alpha^{[0]} = \beta^{[0]} = (\alpha + \beta)^{[0]}$ folgt sofort

$$\sum_{i=0}^0 \binom{0}{i} \alpha^{[i]} \beta^{[0-i]} = 1 = (\alpha + \beta)^{[0]},$$

was den Induktionsanfang erledigt.

Induktionsvoraussetzung: Für beliebiges aber festes $n \in \mathbb{N}$ gelte $(\alpha + \beta)^{[n]} = \sum_{i=0}^n \binom{n}{i} \alpha^{[n-i]} \cdot \beta^{[i]}$.

Induktionsschritt: Sei also n wie in der Induktionsvoraussetzung. Wir beweisen die Aussage nun für $n+1$.

$$\begin{aligned}
(\alpha + \beta)^{[n+1]} &= \prod_{i=0}^n (\alpha + \beta - i) = (\alpha + \beta - n) \cdot \prod_{i=0}^{n-1} (\alpha + \beta - i) \\
&= (\alpha + \beta - n) \cdot (\alpha + \beta)^{[n]} \stackrel{IV}{=} (\alpha + \beta - n) \cdot \sum_{i=0}^n \binom{n}{i} \cdot \alpha^{[i]} \cdot \beta^{[i]} \\
&= \sum_{i=0}^n \underbrace{(\alpha + \beta - n)}_{=(\alpha-i)+(\beta-n+i)} \cdot \binom{n}{i} \cdot \alpha^{[i]} \cdot \beta^{[n-i]} \tag{1.19}
\end{aligned}$$

$$= \sum_{i=0}^n \binom{n}{i} (\alpha - i) \cdot \alpha^{[i]} \cdot \beta^{[n-i]} + \sum_{i=0}^n \binom{n}{i} \cdot \alpha^{[i]} \cdot (\beta - n + i) \cdot \beta^{[n-i]} \tag{1.20}$$

Nur mit der Definition der fallenden Fakultät folgt

$$(\alpha - i) \cdot \alpha^{[i]} = (\alpha - i) \cdot \prod_{j=0}^{i-1} (\alpha - j) = \prod_{j=0}^i (\alpha - j) = \alpha^{[i+1]}$$

und

$$(\beta - n + i) \cdot \beta^{[n-i]} = (\beta - n + i) \cdot \prod_{j=0}^{n-i-1} (\beta - j) = \prod_{j=0}^{n-i} (\beta - j) = \beta^{[n-i+1]}.$$

Setzen wir diese beiden Gleichungen in (1.19) ein, erhalten wir $(\alpha + \beta)^{[n+1]}$

$$\begin{aligned}
&= \sum_{i=0}^n \binom{n}{i} \cdot \alpha^{[i+1]} \cdot \beta^{[n-i]} + \sum_{i=0}^n \binom{n}{i} \cdot \alpha^{[i]} \cdot \beta^{[n+1-i]} \\
&= \binom{n}{n} \cdot \alpha^{[n+1]} \cdot \beta^{[0]} + \sum_{i=0}^{n-1} \binom{n}{i} \cdot \alpha^{[i+1]} \cdot \beta^{[n-i]} + \sum_{i=1}^n \binom{n}{i} \cdot \alpha^{[i]} \cdot \beta^{[n+1-i]} + \binom{n}{0} \cdot \alpha^{[0]} \cdot \beta^{[n+1]} \\
&= \alpha^{[n+1]} \cdot \beta^{[0]} + \sum_{i=1}^n \binom{n}{i-1} \cdot \alpha^{[i]} \cdot \beta^{[n+1-i]} + \sum_{i=1}^n \binom{n}{i} \cdot \alpha^{[i]} \cdot \beta^{[n+1-i]} + \alpha^{[0]} \cdot \beta^{[n+1]} \\
&= \binom{n+1}{0} \alpha^{[n+1]} \cdot \beta^{[0]} + \sum_{i=1}^n \underbrace{\left(\binom{n}{i-1} + \binom{n}{i} \right)}_{\binom{n+1}{i}} \cdot \alpha^{[i]} \cdot \beta^{[n+1-i]} + \binom{n+1}{n+1} \cdot \alpha^{[0]} \cdot \beta^{[n+1]} \\
&= \sum_{i=0}^{n+1} \binom{n+1}{i} \cdot \alpha^{[i]} \cdot \beta^{[n+1-i]}.
\end{aligned}$$

Das war zu zeigen.

Lösung von Aufgabe 126 Seien $n \in \mathbb{N}_0$ und g_n die Anzahl von Lösungen der Gleichung $x_1 + x_2 + x_3 + x_4 = n$ mit den angegebenen Randbedingungen. Wir betrachten

zunächst die recht einfachen Gleichungen $x_i = n$ für $i \in \{1, 2, 3, 4\}$ und $n \in \mathbb{N}$. Die Anzahl der Lösungen von $x_1 = n$ (bzw. $x_2 = n, x_3 = n, x_4 = n$) nennen wir a_n (bzw. b_n, c_n, d_n). Dann sagen die angegebenen Randbedingungen genau

$$\begin{aligned} a_n &= \begin{cases} 1 & , \text{ falls } n \equiv 1 \pmod{4} \\ 0 & \text{sonst} \end{cases} & b_n &= \begin{cases} 1 & , \text{ falls } n \geq 5 \\ 0 & \text{sonst} \end{cases} \\ c_n &= \begin{cases} 1 & , \text{ falls } n \leq 3 \\ 0 & \text{sonst} \end{cases} \end{aligned}.$$

Da es keine Randbedingung an x_4 gibt, ist schlicht $d_n = 1$ für alle $n \in \mathbb{N}_0$. Für alle $r, s, t, u \in \mathbb{N}_0$ ist $a_r b_s c_t d_u \in \{0, 1\}$. Weiter ist $a_r b_s c_t d_u = 1$ genau dann, wenn $r \equiv 1 \pmod{4}$, $s \geq 5$ und $t \leq 3$ gilt. Damit erhalten wir

$$\begin{aligned} \sum_{r+s+t+u=n} a_r b_s c_t d_u &= |\{(r, s, t, u) \in \mathbb{N}_0 | a_r b_s c_t d_u = 1\}| \\ &= |\{(r, s, t, u) \in \mathbb{N}_0 | r + s + t + u = n, r \equiv 1 \pmod{4}, s \geq 5, t \leq 3\}| = g_n. \end{aligned}$$

Das ist also genau die gesuchte Zahl! Sind nun $A(x) = \sum_{n \geq 0} a_n x^n$, $B(x) = \sum_{n \geq 0} b_n x^n$, $C(x) = \sum_{n \geq 0} c_n x^n$ und $D(x) = \sum_{n \geq 0} d_n x^n$, dann ist

$$A(x) \cdot B(x) \cdot C(x) \cdot D(x) = \sum_{n \geq 0} \left(\sum_{r+s+t+u=n} a_r b_s c_t d_u \right) x^n = \sum_{n \geq 0} g_n x^n. \quad (1.21)$$

Wir wollen also die Koeffizienten der formalen Potenzreihe $A(x) \cdot B(x) \cdot C(x) \cdot D(x)$ berechnen. Wir betrachten die formalen Potenzreihen zunächst einzeln:

- $A(x) = \sum_{n \geq 0} x^{4n+1} = x \cdot \sum_{n \geq 0} x^{4n} = \frac{x}{1-x^4}$,
- $B(x) = \sum_{n \geq 5} x^n = x^5 \cdot \sum_{n \geq 0} x^n = \frac{x^5}{1-x}$,
- $C(x) = 1 + x + x^2 + x^3 = \frac{1-x^4}{1-x}$ und
- $D(x) = \sum_{n \geq 0} x^n = \frac{1}{1-x}$.

Damit erhalten wir

$$\begin{aligned} \sum_{n \geq 0} g_n x^n &\stackrel{(1.21)}{=} A(x) \cdot B(x) \cdot C(x) \cdot D(x) = \frac{x}{1-x^4} \cdot \frac{x^5}{1-x} \cdot \frac{1-x^4}{1-x} \cdot \frac{1}{1-x} \\ &= \frac{x^6}{(1-x)^3} = x^6 \cdot \sum_{n \geq 0} \binom{n+2}{n} x^n = \sum_{n \geq 6} \binom{n-4}{n-6} x^n. \end{aligned}$$

Es folgt, $g_n = \begin{cases} 0 & , \text{ falls } n \leq 5 \\ \binom{n-4}{n-6} & , \text{ falls } n \geq 6 \end{cases}$ und die Aufgabe ist gelöst.

Diskrete Mathematik

Ein kompakter Einstieg

Pottmeyer, L.

2019, XVI, 226 S. 47 Abb., 15 Abb. in Farbe., Softcover

ISBN: 978-3-662-59662-3