Übungsblatt 1

Aufgabe 1

In dieser Aufgabe werden weitere Regeln für das Rechnen mit Ungleichungen aufgestellt. Beim Beweis dürfen **nur** solche Regeln benutzt werden, die in der Vorlesung als Grundregeln aufgestellt oder darauf basierend bewiesen wurden. Andere Regeln, die (vielleicht noch aus der Schulzeit) bekannt sind, dürfen **nicht** benutzt werden.

(a) Behauptung: $0 < x < y \Longrightarrow x^{-1} > y^{-1} > 0$

Beweis. $0 < x < y$ bedeutet $0 < x$ und $x < y$. Da $<$ transitiv ist, folgt insbesondere auch $0 < y$.
Als ersten Schritt beweisen wir: $x > 0 \Longrightarrow x^{-1} > 0$. Dazu gehen wir indirekt vor:
Annahme:
(1) $x^{-1} \leq 0$.
Da $x > 0$ ist, können wir wegen O_M) die Ungleichung (1) mit x multiplizieren.

$$x^{-1} \leq 0 \mid \cdot x \Longrightarrow 1 = x^{-1}x \leq 0 \cdot x = 0 \Longrightarrow 1 \leq 0$$

Dies ist aber ein *Widerspruch*, da $1 > 0$ gilt. Folglich ist die Annahme falsch und unsere erste Behauptung bewiesen.
Wegen $x^{-1} > 0$ folgt mit (1.8a) ii):

$$x < y \mid \cdot x^{-1} \Longrightarrow x \cdot x^{-1} < y \cdot x^{-1} \Longrightarrow 1 < y \cdot x^{-1}$$

Nach dem ersten Schritt gilt auch $y^{-1} > 0$, so daß wir wieder mit (1.8a) ii) schließen können.

$$1 < yx^{-1} \mid \cdot y^{-1} \Longrightarrow y^{-1} = y^{-1} \cdot 1 < y^{-1}(yx^{-1}) = (y^{-1}y)x^{-1} = 1 \cdot x^{-1} = x^{-1}$$

Also gilt $y^{-1} < x^{-1}$, und das war zu zeigen. □

Bemerkung: Die Voraussetzung $0 < x < y$ ist erforderlich: $-3 < -2$, aber $-1/3 > -1/2$
Fazit: Geht man in einer Ungleichung zwischen positiven reellen Zahlen zu den inversen Elementen über, so dreht sich das Ungleichheitszeichen um.

(b) Behauptung: $x < y \ \wedge \ w < z \Longrightarrow x + w < y + z$.

Beweis. Die folgenden Überlegungen basieren auf (1.8a), i) und iii):

$$\left.\begin{array}{l} x < y \mid + w \Longrightarrow x + w < y + w \\ w < z \mid + y \Longrightarrow y + w < y + z \end{array}\right\} \Longrightarrow x + w < y + z$$

Damit ist die Behauptung bewiesen. □

Fazit: Strikte Ungleichungen dürfen addiert werden.

(c) Behauptung: $x \geq 0,\ y \geq 0,\ x^2 \leq y^2 \Longrightarrow x \leq y$

Beweis. 1. Fall: $x = 0$ oder $y = 0$. Hier folgt die Behauptung unmittelbar.
Die Voraussetzung im 1. Fall ist von der Form $A \vee B$. Die Negation hiervon ist dann $\neg A \wedge \neg B$ (Regel von de Morgan). Also:
2. Fall: $x > 0$ und $y > 0$. Wir führen einen indirekten Beweis. Die Negation der Behauptung $x \leq y$ ist dann $x > y$. Wir benutzen wieder (1.8).
Annahme: $x > y$.

$$\left.\begin{array}{l} x > y \mid \cdot x \Longrightarrow x^2 = x \cdot x > y \cdot x \\ x > y \mid \cdot y \Longrightarrow y \cdot x > y \cdot y = y^2 \end{array}\right\} \Longrightarrow x^2 > y^2$$

Damit erhalten wie einen *Widerspruch* zu unserer Voraussetzung $x^2 \leq y^2$. □

Bemerkung: Die Voraussetzung $x \geq 0,\ y \geq 0$ ist erforderlich: Für $x = -3$ und $y = -4$ gilt zwar $x^2 = (-3)^2 = 9 \leq 16 = (-4)^2 = y^2$, aber $x = -3 > -4 = y$.

Fazit: Aus einer Ungleichung zwischen nichtnegativen Zahlen darf auf beiden Seiten die Wurzel gezogen werden (dies entspricht dem Übergang von x^2 nach x):

$$x \geq 0,\ y \geq 0,\ x \leq y \Longrightarrow \sqrt{x} \leq \sqrt{y}.$$

(d) Behauptung: $0 < x < y \Longrightarrow x^2 < y^2$

Beweis. Wir führen wieder einen indirekten Beweis:
Annahme: $x^2 \geq y^2$ (Dies ist die Negation von $x^2 < y^2$) Nach dem Aufgabenteil c) (wir dürfen dieses Ergebnis jetzt benutzen, da wir es gerade bewiesen haben!) folgt $x \geq y$ im *Widerspruch* zu unserer Voraussetzung $x < y$. □

Bemerkung: Die Voraussetzung $0 < x < y$ ist erforderlich: Es gilt zwar $-3 < -2$, aber $(-3)^2 = 9 > 4 = (-2)^2$.
Fazit: Eine Ungleichung zwischen positiven reellen Zahlen darf quadriert werden.

Aufgabe 2

(a) Zu zeigen: Für alle $x \in \mathbb{R}$ gilt: $\lfloor -x \rfloor = -\lceil x \rceil$

Beweis. Setze $m := \lfloor -x \rfloor$. Dann ist nach Satz (1.10) $m \leq -x < m+1$. Multiplikation mit -1 liefert $-m \geq x > -(m+1) = -m-1$. Nach Satz (1.11) ist dann $-m = \lceil x \rceil$. $\Longrightarrow \lfloor -x \rfloor = m = -\lceil x \rceil$. □

(b) Zu zeigen: Für alle $x \in \mathbb{R}, n \in \mathbb{Z}$ gilt: $\lfloor x+n \rfloor = \lfloor x \rfloor + n$.

Beweis. Setze $m := \lfloor x+n \rfloor$, dann ist nach (1.10) $m \leq x+n < m+1$. Durch Addition von $-n$ erhält man $m-n \leq x < m-n+1$. Also ist $m-n = \lfloor x \rfloor$ und somit $\lfloor x+n \rfloor - n = m-n = \lfloor x \rfloor$. Addition von n auf beiden Seiten liefert schließlich $\lfloor x+n \rfloor = \lfloor x \rfloor + n$. □

(c) Behauptung: Die Formel $\lfloor n \cdot x \rfloor = \lfloor x \rfloor \cdot n$ ist nicht für alle $x \in \mathbb{R}, n \in \mathbb{Z}$ richtig.

Beweis. Gegenbeispiel: $n = 5, x = \frac{1}{2}$:

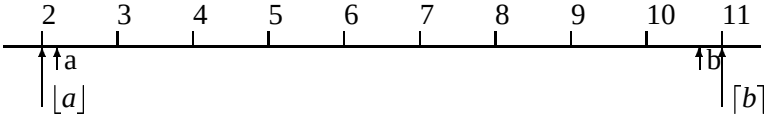
$$\left\lfloor 5 \cdot \frac{1}{2} \right\rfloor = \left\lfloor \frac{5}{2} \right\rfloor = 2$$

$$5 \cdot \left\lfloor \frac{1}{2} \right\rfloor = 5 \cdot 0 = 0$$

Aber $0 \neq 2$, also $\left\lfloor 5 \cdot \frac{1}{2} \right\rfloor \neq 5 \cdot \left\lfloor \frac{1}{2} \right\rfloor$. □

(d) Zu zeigen: Für $a, b \in \mathbb{R}$ gilt: Die Anzahl der ganzen Zahlen in $]a,b[$ ist $\lceil b \rceil - \lfloor a \rfloor - 1$.

Beweis. Zunächst ein kleines Bild zur Veranschaulichung des Aussage für $a = 2.2,\ b = 10.7$:



Sei $n \in]a,b[$ eine ganze Zahl. Es gilt

$$a < n \Longrightarrow \lfloor a \rfloor \leq a < n \Longrightarrow \lfloor a \rfloor + 1 \leq n$$

$$n < b \Longrightarrow n < b \leq \lceil b \rceil \Longrightarrow n \leq \lceil b \rceil - 1$$

und damit

(2) $\lfloor a \rfloor + 1 \leq n \leq \lceil b \rceil - 1$.

Seien $x, y \in \mathbb{Z}$ mit $x \leq y$. Die Anzahl der ganzen Zahlen im abgeschlossenen Intervall $[x,y]$ ist $y-x+1$; denn: $x+0, x+1, x+2, \ldots, x+(y-x) \in [x,y]$ sind alle ganzen Zahlen in $[x,y]$.

Mit (2) folgt für die Anzahl der ganzen Zahlen in $]a,b[$:

$$\lceil b\rceil - 1 - (\lfloor a\rfloor + 1) + 1 = \lceil b\rceil - 1 - \lfloor a\rfloor - 1 + 1 = \underline{\lceil b\rceil - \lfloor a\rfloor - 1}.$$

□

Aufgabe 3

Gesucht ist die Zahl der Bits (= Stellen, die jeweils 0 oder 1 sein können), die benötigt werden, um $n = 76543210$ darzustellen.
Nach (1.13) ist die Zahl der Binärstellen von n gleich $\lfloor \log_2(n)\rfloor + 1$. (Dabei ist $\log_2(n) = \frac{\ln(n)}{\ln(2)}$, wobei ln der natürliche Logarithmus, also zur Basis $e = 2.71828\ldots$, ist.)
Wir erhalten $\lfloor \log_2(n)\rfloor + 1 = \lfloor 26.18977107\ldots\rfloor + 1 = 26 + 1 = 27$, benötigen also 27 Stellen, um n binär darzustellen.

$$n = (76543210)_{10} = (10010001111111110100111010 10)_2$$

Übungsblatt 2

Aufgabe 4

Zu zeigen: Für $x \in \mathbb{R}$ gilt: $\lceil x\rceil - \lfloor x\rfloor = \begin{cases} 1 & \text{falls } x \notin \mathbb{Z} \\ 0 & \text{sonst.} \end{cases}$

Beweis. 1. Fall: $x \in \mathbb{Z}$. Dann ist $\lfloor x\rfloor = \lceil x\rceil = x$ und somit $\lceil x\rceil - \lfloor x\rfloor = 0$.
2. Fall: $x \notin \mathbb{Z}$. Nach (1.11) gilt $n = \lceil x\rceil \iff n - 1 < x \le n$. Wegen $x \notin \mathbb{Z}$, muß $n \neq x$ gelten, und die Ungleichung verschärft sich zu $n - 1 < x < n$. Addition von 1 liefert $n < x + 1 < n + 1$, nach (1.10) und Übungsaufgabe 2c folgt $n = \lfloor x + 1\rfloor = \lfloor x\rfloor + 1$.
Also ist $\lfloor x\rfloor = \lceil x\rceil + 1 \Longrightarrow \lceil x\rceil - \lfloor x\rfloor = 1$. □

Aufgabe 5

Zu zeigen: Die Dreiecksungleichung $|x+y| \le |x| + |y|$.

Beweis. 1. Fall: $x + y \ge 0$. Dann ist $|x+y| = x + y \le |x| + |y|$. Die letzte Ungleichung folgt aus $x \le |x|$ und $y \le |y|$ (1.15d).
2. Fall: $x + y < 0$. Nach der Definition von $|\cdot|$ gilt jetzt

$$|x+y| = -(x+y) = (-x) + (-y) \le |-x| + |-y| = |x| + |y|\,.$$

Hier haben wir (1.15d) und (1.15c) benutzt. Wir haben also gezeigt:

Für alle $x, y \in \mathbb{R}$: $|x+y| \le |x| + |y|\,.$

□

Aufgabe 6

Zu zeigen: $P \wedge Q \Longrightarrow P$ ist allgemeingültig, also $(P \wedge Q \Longrightarrow P) \iff W$.

Beweis. Wir stellen die Wahrheitstafel für $P \wedge Q \Longrightarrow P$ auf:

P	Q	$P \wedge Q$	$P \wedge Q \Longrightarrow P$
W	W	W	W
W	F	F	W
F	W	F	W
F	F	F	W

und sehen, daß die Formel für alle Belegungen von P und Q wahr ist. Und so kann man das formal nachrechnen:

$$\begin{aligned}
((P \wedge Q) \Longrightarrow P) &\Longleftrightarrow \neg(P \wedge Q) \vee P && \text{nach (2.4c)}\\
&\Longleftrightarrow (\neg P \vee \neg Q) \vee P && \text{nach (2.3f)}\\
&\Longleftrightarrow (\neg P \vee P) \vee (\neg Q) && \text{nach (2.3d,e)}\\
&\Longleftrightarrow W \vee (\neg Q) && \text{nach (2.3a)}\\
&\Longleftrightarrow W && \text{nach Definition von } \vee
\end{aligned}$$

Wir erhalten also auch hier $(P \wedge Q \Longrightarrow P) \Longleftrightarrow W$. □

Aufgabe 7

Das Symbol $|$ wird auch nand genannt, also *nicht und.*

(a)

A	B	$\neg(A \wedge B)$
W	W	F
W	F	W
F	W	W
F	F	W

(b) (i) Zu zeigen: $A|A$ ist logisch äquivalent zu $\neg A$, also $A|A \Longleftrightarrow \neg A$

Beweis. $A|A \Longleftrightarrow \neg(A \wedge A) \Longleftrightarrow \neg A$, denn $A \wedge A \Longleftrightarrow A$. □

(ii) Zu zeigen: $(A|B)|(A|B) \Longleftrightarrow A \wedge B$.

Beweis. $(A|B)|(A|B) \overset{\text{(i)}}{\Longleftrightarrow} \neg(A|B) \overset{\text{Def.}}{\Longleftrightarrow} \neg\neg(A \wedge B) \Longleftrightarrow A \wedge B$. □

(c) Gesucht ist eine zu $(A \Longrightarrow B)$ äquivalente Formel, in der nur $|$ vorkommt.
Wir wissen $(A \Longrightarrow B) \Longleftrightarrow (\neg A \vee B)$. Die Formel für $|$ liefert uns

$(A|B) \Longleftrightarrow \neg(A \wedge B) \Longleftrightarrow (\neg A \vee \neg B)$.

Um die richtige Formel zu erhalten, müssen wir also noch B negieren. Nach Teil b(i) dieser Aufgabe kann dies durch $(B|B)$ erreicht werden, und wir erhalten:

$(A|(B|B)) \overset{\text{Def.}}{\Longleftrightarrow} \neg(A \wedge (B|B)) \overset{\text{b(ii)}}{\Longleftrightarrow} \neg(A \wedge \neg B) \Longleftrightarrow (\neg A \vee B) \Longleftrightarrow (A \Longrightarrow B)$.

Aufgabe 8

Es ist das *Archimedische Axiom* mit Hilfe von Quantoren zu formulieren:

$\forall x \in \mathbb{R}\ \exists n \in \mathbb{N} : n > x$

Die Negation liefert:

$\exists x \in \mathbb{R}\ \forall n \in \mathbb{N} : n \leq x$

man sieht, daß die Quantoren "umklappen", und die Aussage (rechts von ":") negiert wird.

Übungsblatt 3

Aufgabe 9

(a) Die Menge der Buchstaben des Wortes "Mathematik" ist $\{M, a, t, h, e, m, i, k\}$ oder – wenn man Groß-/Kleinschreibung nicht berücksichtigt –: $\{m, a, t, h, e, i, k\}$. Wie man sieht, kommt ein

Element in einer Menge nur einmal vor. Dabei spielt die Reihenfolge der Buchstaben in der Menge *keine* Rolle.

(b) Gesucht ist eine *intensionale* Darstellung der Menge $M = \{1, 2, 4, 8, 16, 32, \dots\}$, also mit Hilfe eines geeigneten Prädikates.
Man sieht leicht, daß die Elemente von M gerade die Zweierpotenzen sind: $1 = 2^0,\ 2 = 2^1,\ 4 = 2^2,\ \dots$. Damit erhält man $M = \{x \mid\ x \in \mathbb{N}, \exists n \in \mathbb{N}_0 :\ x = 2^n\}$.

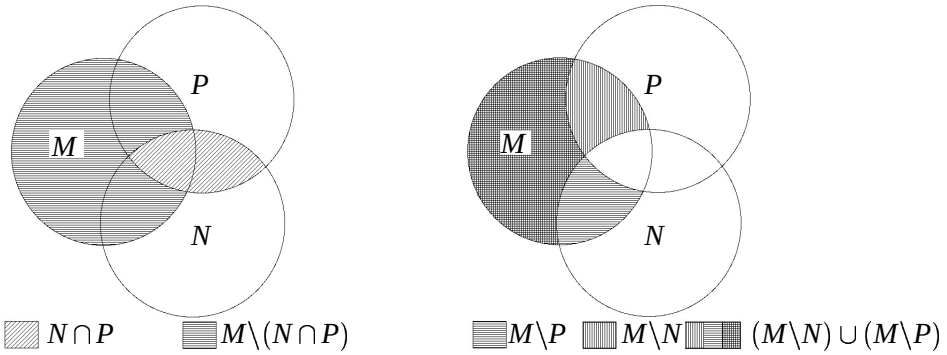
(c) Seien $M,\ N$ und P die Mengen der gazzahligen Vielfachen von $6,\ 8$ bzw. 48. Gesucht sind Beschreibungen der Mengen mit Prädikaten.

$$M = \{x \mid\ x \in \mathbb{Z} \wedge \exists k \in \mathbb{Z} :\ x = k \cdot 6\}$$
$$N = \{y \mid\ y \in \mathbb{Z} \wedge \exists k \in \mathbb{Z} :\ y = k \cdot 8\}$$
$$P = \{z \mid\ z \in \mathbb{Z} \wedge \exists k \in \mathbb{Z} :\ z = k \cdot 48\}$$

Es gilt $M \cap N \neq P$, denn $24 = 4 \cdot 6 = 3 \cdot 8 \in M \cap N$, aber $24 \notin P$.

Aufgabe 10

(a)



(b) Zu zeigen: $M\backslash(N \cap P) = (M\backslash N) \cup (M\backslash P)$.

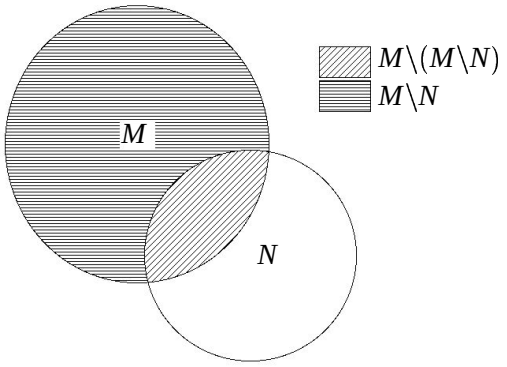
Beweis. Um die Gleichheit zu zeigen, muß folgendes nachgerechnet werden:
$\forall x : x \in M\backslash(N \cap P) \iff x \in (M\backslash N) \cup (M\backslash P)$.
Dazu betrachten wir ein beliebiges x:

$$\begin{aligned}
x \in M\backslash(N \cap P) &\iff x \in M \wedge x \notin (N \cap P) && \text{(Definition von } \backslash) \\
&\iff x \in M \wedge \neg(x \in N \wedge x \in P) \\
&\iff x \in M \wedge (x \notin N \vee x \notin P) && \text{(de Morgan)} \\
&\iff (x \in M \wedge x \notin N) \vee (x \in M \wedge x \notin P) && \text{(Distributivgesetz)} \\
&\iff x \in (M\backslash N) \vee x \in (M\backslash P) \\
&\iff x \in (M\backslash N) \cup (M\backslash P)
\end{aligned}$$

□

Aufgabe 11

(a) Die Veranschaulichung von $M\backslash(M\backslash N)$:



Die Vermutung: $M\backslash(M\backslash N) = M \cap N$.

(b) Zu zeigen: $M\backslash(M\backslash N) = M \cap N$.

Beweis. Wir betrachten ein beliebiges Element x:

$$
\begin{aligned}
x \in M\backslash(M\backslash N) &\iff x \in M \wedge \neg x \in (M\backslash N) && \text{(Definition von } \backslash) \\
&\iff x \in M \wedge \neg(x \in M \wedge x \notin N) \\
&\iff x \in M \wedge (x \notin M \vee x \in N) && \text{(de Morgan)} \\
&\iff (\underbrace{x \in M \wedge x \notin M}_{\iff F}) \vee (x \in M \wedge x \in N) && \text{(Distributivgesetz)} \\
&\iff x \in M \wedge x \in N && (F \vee A \iff A) \\
&\iff x \in M \cap N && \text{(Definition von } \cap)
\end{aligned}
$$

□

Aufgabe 12

Sei $M = \{1,2\}$, gesucht ist $\mathcal{P}(\mathcal{P}(M))$.
Zunächst bestimmen wir $\mathcal{P}(M) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$, und erhalten:

$$
\begin{aligned}
\mathcal{P}(\mathcal{P}(M)) = \{&\emptyset,\ \{\emptyset\},\ \{\{1\}\},\ \{\{2\}\},\ \{\{1,2\}\}, \\
&\{\emptyset,\{1\}\},\ \{\emptyset,\{2\}\},\ \{\emptyset,\{1,2\}\},\ \{\{1\},\{2\}\},\ \{\{1\},\{1,2\}\},\ \{\{2\},\{1,2\}\}, \\
&\{\emptyset,\{1\},\{2\}\},\ \{\emptyset,\{1,2\},\{2\}\},\ \{\emptyset,\{1\},\{1,2\}\},\ \{\{1\},\{2\},\{1,2\}\}, \\
&\{\emptyset,\{1\},\{2\},\{1,2\}\}\ \}
\end{aligned}
$$

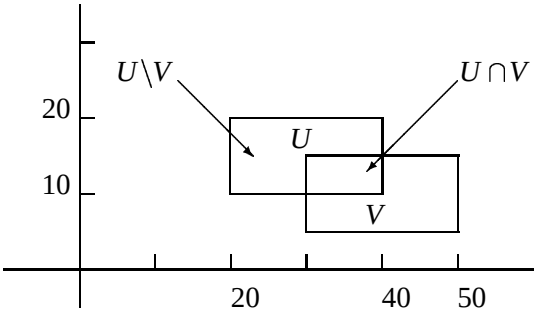
Es sind genau 16 Elemente.

Aufgabe 13

Gegeben sind die zwei Mengen

$$U := \big\{(x,y) \,\big|\, (x,y) \in \mathbb{Z} \times \mathbb{Z},\ 20 \le x \le 40,\ 10 \le y \le 20\big\}$$
$$V := \big\{(x,y) \,\big|\, (x,y) \in \mathbb{Z} \times \mathbb{Z},\ 30 \le x \le 50,\ 5 \le y \le 15\big\}$$

(a) Zunächst eine graphische Veranschaulichung:



Wie man schon an der Graphik sieht, ist $V \not\subseteq U$, z.B. ist $(50,5) \in V$, aber $(50,5) \notin U$.
Die Menge U kann dargestellt werden als:

$$U = \{20,21,22,\ldots,39,40\} \times \{10,11,12,\ldots,19,20\}$$

und man sieht, daß U $21 \cdot 11 = 321$ Elemente hat.

(b) Die Schnittmenge berechnet sich – wie man an der Graphik schon sieht – zu

$$U \cap V = \big\{(x,y) \,\big|\, (x,y) \in \mathbb{Z} \times \mathbb{Z},\ 30 \le x \le 40,\ 10 \le y \le 15\big\}.$$

Analog ist die Differenzmenge:

$$U \backslash V = \big\{(x,y) \,\big|\, (x,y) \in \mathbb{Z} \times \mathbb{Z},\ 20 \le x \le 30,\ 10 \le y \le 20\big\}$$
$$\cup \big\{(x,y) \,\big|\, (x,y) \in \mathbb{Z} \times \mathbb{Z},\ 30 \le x \le 40,\ 15 \le y \le 20\big\}.$$

Übungsblatt 4

Aufgabe 14

Wir betrachten die Relation $R \subseteq \mathbb{N} \times \mathbb{N}$, die für $(m,n),(m',n') \in \mathbb{N} \times \mathbb{N}$ definiert ist durch:
(3) $\quad (m,n)R(m',n') :\Longleftrightarrow m \le m' \wedge n \le n'$.

(a) Zu zeigen: R ist eine partielle Ordnung auf $\mathbb{N} \times \mathbb{N}$.

Beweis. Reflexivität: Sei also $(m,n) \in \mathbb{N} \times \mathbb{N}$ beliebig gewählt. Dann gilt $m \le m \wedge n \le n$, da $\le$ reflexiv ist. Also ist wegen (3) $(m,n)R(m,n)$, und damit ist R reflexiv.
Antisymmetrie: Seien $(m,n),\ (m',n') \in \mathbb{N} \times \mathbb{N}$ mit $(m,n)R(m',n')$ und $(m',n')R(m,n)$. Das heißt doch nach (3), daß

$$m \le m' \wedge n \le n' \text{ und } m' \le m \wedge n' \le n.$$

Da aber $\le$ antisymmetrisch ist, folgen $m = m'$ und $n = n'$. Zusammengefaßt heißt das: $(m,n)R(m',n') \wedge (m',n')R(m,n) \Longrightarrow m = m' \wedge n = n' \Longrightarrow (m,n) = (m',n')$. Das ist aber genau die Definition von antisymmetrisch.
Transitivität: Seien $(m,n),\ (m',n'),(m'',n'') \in \mathbb{N} \times \mathbb{N}$ beliebig mit $(m,n)R(m',n')$ und $(m',n')R(m'',n'')$. Dann gelten nach (3):

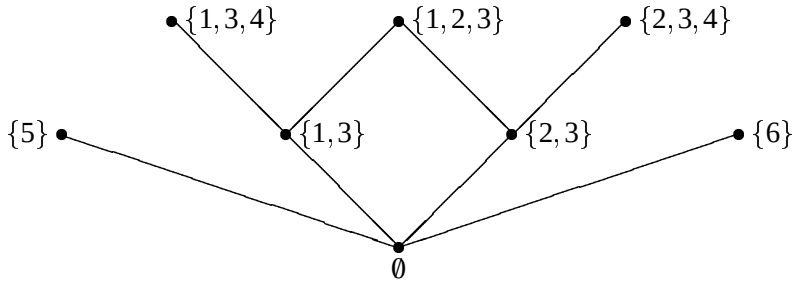
$$m \le m' \wedge n \le n' \text{ und } m' \le m'' \wedge n' \le n''.$$

Da $\le$ transitiv ist, folgen $m \le m''$ und $n \le n''$. Also $(m,n)R(n'',m'')$. Wir haben also gezeigt: $(m,n)R(m',n') \wedge (m',n')R(m'',n'') \Longrightarrow (m,n)R(n'',m'')$. Damit ist R transitiv.
Aus den Eigenschaften *reflexiv, antisymmetrisch* und *transitiv* folgt, daß R eine partielle Ordnungsrelation ist. □

Behauptung: R ist nicht linear.

Beweis. Linearität heißt $\forall (m,n),(m',n') \in \mathbb{N} \times \mathbb{N} :\ (m,n)R(m',n') \vee (m',n')R(m,n)$. Es reicht also ein Gegenbeispiel anzugeben:
Es gilt $(1,2) \not R (2,1)$ und $(2,1) \not R (1,2)$. Also ist R nicht linear. □

(b) Zu $M := \{\emptyset, \{5\}, \{6\}, \{1,3\}, \{2,3\}, \{1,2,3\}, \{1,3,4\}, \{2,3,4\}\}$ ist das Hasse-Diagramm bezüglich der Relation $\subseteq$ aufzustellen:



Wie man sieht, ist $\emptyset$ das kleinste Element der Menge, denn $\forall x \in M : \emptyset \subseteq x$. Damit ist $\emptyset$ auch das einzige minimale Element. Es gibt kein größtes Element; denn $\forall x \in M\ \exists y \in M : y \not\subseteq x$.
Die maximalen Elemente in $(M, \subseteq)$ sind: $\{5\},\ \{6\},\ \{1,2,3\},\ \{1,3,4\},\ \{2,3,4\}$.
$(M, \subseteq)$ ist nicht linear geordnet, denn z.B. $\{1,3\} \not\subseteq \{2,3\}$ und $\{2,3\} \not\subseteq \{1,3\}$.

Aufgabe 15

Die Relation R ist auf der Menge $M = \{a,b,c,d,e\}$ durch die untenstehende Tabelle definiert:

R	a	b	c	d	e
a	1	0	1	0	1
b	0	1	0	1	0
c	1	0	1	0	1
d	0	1	0	1	0
e	1	0	1	0	1

(a) Zu zeigen: R ist eine Äquivalenzrelation auf M.

Beweis. Reflexivität: Es gilt $\forall x \in M : xRx$, da in der Hauptdiagonalen nur 1en stehen.
Symmetrie: Es gilt $\forall x,y \in M : xRy \Longrightarrow yRx$, da die Tabelle symmetrisch zur Hauptdiagonalen ist.
Transitivität: Behauptung: $\forall x,y,z \in R : xRy \wedge yRx \Longrightarrow xRy$.
Die Behauptung ist aufgrund der Reflexivität und Symmetrie von R richtig, wenn mindestens zwei der x,y,z gleich sind.
Es bleibt also der Fall paarweise verschiedener x,y,z zu betrachten. Wir listen nun alle x,y,z auf, für die $xRy \wedge yRz$ gelten kann:

x	y	z	xRz	x	y	z	xRz	x	y	z	xRz	x	y	z	xRz
a	c	e	1	c	e	a	1	a	e	c	1	d	b	–	–
b	d	–	–	e	a	c	1	c	a	e	1	e	c	a	1

Wie man sieht, ist die Transitivität offensichtlich erfüllt. □

(b) Gesucht sind die Äquivalenzklassen $[x]_R$ von allen Elementen $x \in M$. Definiert sind die Äquivalenzklassen durch $[x]_R = \{y \mid y \in M, xRy\}$.

$[a]_R = \{a,c,e\}$ $\quad$ $[b]_R = \{b,d\}$

$[c]_R = \{a,c,e\}$ $\quad$ $[d]_R = \{b,d\}$

$[e]_R = \{a,c,e\}$ $\quad$ $+$

Wie man sofort sieht, gelten $[a]_R = [c]_R = [d]_R$ und $[b]_R = [c]_R$. Damit ist

$M/R = \{[a]_R, [b]_R\} = \{\{a,c,e\},\ \{b,d\}\}$.

Aufgabe 16

Auf der Menge $M = \{a,b,c,d\}$ soll eine Relation R definiert werden, die reflexiv und symmetrisch, aber nicht transitiv ist.
Dazu definieren wir

R	a	b	c	d
a	1	1	0	1
b	1	1	1	1
c	0	1	1	1
d	1	1	1	1

R ist reflexiv, da auf der Hauptdiagonalen nur 1en stehen. R ist symmetrisch, da die Tabelle symmetrisch zur Hauptdiagonalen ist. R ist nicht transitiv, denn $aRb \wedge bRc$, aber $a \not R c$.

Aufgabe 17

Die Relation R auf der Menge $\mathbb{R} \times \mathbb{R}$ ist definiert durch:

$$(x,y)R(x',y') :\Longleftrightarrow x - x' = y - y'.$$

(a) Zu zeigen: R ist eine Äquivalenzrelation auf $\mathbb{R} \times \mathbb{R}$.

Beweis. Reflexivität: $x - x = 0 = y - y \Longrightarrow (x,y)R(x,y)$.
Symmetrie: $(x,y)R(x',y') \Longrightarrow x - x' = y - y'$. Multipliziert man diese Gleichung mit (-1), so erhält man $-(x-x') = -(y-y') \Longrightarrow x' - x = y' - y \Longrightarrow (x',y')R(x,y)$.
Transitivität: Es gelte, $(x,y)R(x',y')$ und $(x',y')R(x'',y'')$. Damit gelten $x - x' = y - y'$ und $x' - x'' = y' - y''$. Addiert man beide Gleichungen, so erhält man

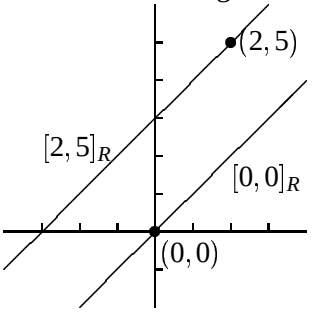
$$\underbrace{(x-x') + (x'-x'')}_{=x-x''} = \underbrace{(y-y') + (y'-y'')}_{y-y''}.$$

also $(x,y)R(x'',y'')$. □

(b) Gesucht sind die Äquivalenzklassen von $(0,0)$ und $(2,5)$.

$$\begin{aligned}
[(0,0)]_R &= \{(x,y) \mid (x,y) \in \mathbb{R} \times \mathbb{R}, (x,y)R(0,0)\} \\
&= \{(x,y) \mid (x,y) \in \mathbb{R} \times \mathbb{R}, x - 0 = y - 0\} \\
&= \{(x,y) \mid (x,y) \in \mathbb{R} \times \mathbb{R}, x = y\} \\
&= \{(x,x) \mid x \in \mathbb{R}\} \\
&= \Delta_R \subseteq \mathbb{R} \times \mathbb{R} \qquad \text{und} \\
[(2,5)]_R &= \{(x,y) \mid (x,y) \in \mathbb{R} \times \mathbb{R}, (x,y)R(2,5)\} \\
&= \{(x,y) \mid (x,y) \in \mathbb{R} \times \mathbb{R}, x - 2 = y - 5\} \\
&= \{(x,y) \mid (x,y) \in \mathbb{R} \times \mathbb{R}, x + 3 = y\} \\
&= \{(x,x+3) \mid x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}
\end{aligned}$$

Wie man sieht, ist $[(0,0)]_R$ eine Gerade durch $(0,0)$ mit Steigung 1. $[(2,5)]_R$ ist eine Gerade durch $(2,5)$ mit Steigung 1.
Grafische Veranschaulichung:



Übungsblatt 5

Aufgabe 18

(a) Sei M eine Menge und $\mathcal{Z} \subseteq \mathcal{P}(M)$ eine Zerlegung von M. Die Relation R sei für $x,y \in M$ definiert durch: $xRy :\Longleftrightarrow \exists Z \in \mathcal{Z} : x \in Z \wedge y \in Z$.
(i) Zu zeigen: R ist eine Äquivalenzrelation auf M.

Beweis. Wir fassen zunächst die Eigenschaften einer Zerlegung zusammen:

1. $\forall Z \in \mathcal{Z} : Z \subseteq M$ und $Z \neq 0$,
2. $\forall Z, Z' \in \mathcal{Z} : Z \neq Z' \Longrightarrow Z \cap Z' = \emptyset$,
3. $M = \bigcup_{Z \in \mathcal{Z}} Z$.

Reflexivität: Sei $x \in M$ beliebig. Dann ist nach 3. $x \in \bigcup_{Z \in \mathcal{Z}} Z$ und somit $x \in Z'$ für ein $Z' \in \mathcal{Z}$. Und damit ist $x \in Z' \wedge x \in Z'$, also xRx.
Symmetrie: Seien $x,y \in M$ mit xRy beliebig. Dann gibt es nach Definition ein $Z' \in \mathcal{Z}$ mit $x \in Z' \wedge y \in Z'$. Da $\wedge$ kommutativ ist, folgt $y \in Z' \wedge x \in Z'$ und somit yRx.
Transitivität: Seien $x,y,z \in M$ beliebig mit xRy und yRz. Dann gilt: $(\exists Z \in \mathcal{Z} : x \in Z \wedge y \in Z)$ und $(\exists Z' \in \mathcal{Z} : y \in Z' \wedge z \in Z')$. Damit ist $y \in Z \cap Z'$ und nach 2. folgt $Z = Z'$. Also $x \in Z \wedge z \in Z$ und damit xRz. □

(ii) Gesucht ist die Äquivalenzklasse eines beliebigen Elements.
Für $x \in M$ ist $[x]_R = \{y \mid y \in M,\ yRx\} = \{y \mid y \in M,\ \exists Z \in \mathcal{Z} : x \in Z \wedge y \in Z\}$. Wie man aus 2. sieht, gibt es *genau ein* $Z' \in \mathcal{Z}$ mit $x \in Z'$. Behauptung: $[x]_R = Z'$ mit diesem Z'.

Beweis. "$\subseteq$": Ist $y \in [x]_R$, so gilt $xRy \Longrightarrow \exists Z \in \mathcal{Z} : x \in Z \wedge y \in Z$, damit ist $Z = Z'$ und $y \in Z'$.
"$\supseteq$": Gelten $y \in Z' \wedge x \in Z'$, so gilt yRx und damit $y \in [x]_R$. □

(b) Gesucht sind alle Äquivalenzrelationen auf $M = \{a,b,c,d\}$.
Ist R eine Äquivalenzrelation auf M, so ist nach (4.10) M/R eine Zerlegung von M. Umgekehrt bestimmt nach (a) jede Zerlegung $\mathcal{Z}$ eine Äquivalenzrelation auf M, deren Äquivalenzklassen gerade die Elemente von $\mathcal{Z}$ sind. Um alle Äquivalenzrelationen auf M zu bestimmen, braucht man daher nur alle möglichen Zerlegungen von M zu finden:

$\lvert\mathcal{Z}\rvert$	Zerlegungen	#Zerlegungen
1	M	1
2	$\{\{a\},\{b,c,d\}\},\ \{\{b\},\{a,c,d\}\},\ \{\{c\},\{a,b,d\}\},$ $\{\{d\},\{a,b,c\}\}$	4
	$\{\{a,b\},\{c,d\}\},\ \{\{a,c\},\{b,d\}\},\ \{\{a,d\},\{b,c\}\}$	3
3	$\{\{a\},\{b\},\{c,d\}\},\ \{\{a\},\{c\},\{b,d\}\},\ \{\{a\},\{d\},\{b,c\}\},$ $\{\{b\},\{c\},\{a,d\}\},\ \{\{b\},\{d\},\{a,c\}\},\ \{\{c\},\{d\},\{a,b\}\}$	6
4	$\{\{a\},\{b\},\{c\},\{d\}\}$	1
Summe		15

Aufgabe 19

(a) Die Abbildung $f : \{a,b,c,d,e\} \to \{1,2,3,4,5,6,7\}$ ist definiert durch
$a \mapsto 2$ $b \mapsto 5$ $c \mapsto 7$
$d \mapsto 3$ $e \mapsto 5$.
Gesucht ist zu $U := \{b,c,d,e\}$ die Bildmenge $f(U)$:
$f(U) = \{f(x) \mid x \in U\} = \{f(b), f(c), f(d), f(e)\} = \{3,5,7\}$,

zu $V := \{3,4,5\}$ die Urbildmenge $f^{-1}(V)$:
$$f^{-1}(V) = \{x \mid x \in M, f(x) \in V\} = \{x \mid x \in M, f(x) \in \{3,4,5\}\} = \{b,d,e\}$$
und zu $V' := \{1,2\}$ die Urbildmenge $f^{-1}(V')$:
$$f^{-1}(V') = \{x \mid x \in M, f(x) \in V'\} = \{x \mid x \in M, f(x) \in \{1,2\}\} = \{a\}.$$

(b) Die Abbildung $g : \mathbb{Z} \to \mathbb{Z}$ ist definiert durch $g(z) = z^2$ für alle $z \in \mathbb{Z}$. Weiter sind $U := \{-2,1,0,1,2,3\}$ und $V := \{-1,3,4,5,9\}$.
$$g(U) = \{g(-2), g(1), g(0), g(1), g(2), g(3)\} = \{0,1,4,9\}$$
$$g^{-1}(U) = \{x \mid x \in \mathbb{Z}, g(x) \in V\} = \{-3,-2,2,3\}$$

Aufgabe 20

Gegeben sind die zwei Abbildungen

$$\begin{array}{rcl} f : \mathbb{R}\times\mathbb{R} & \longrightarrow & \mathbb{R} \\ (r,s) & \longmapsto & r-s \end{array} \qquad \begin{array}{rcl} g : \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & x^3 - x + 1 \end{array}$$

(i) Zu berechnen:
$$(g \circ f)((5,2)) = g(f((5,2)) = g(5-2) = g(3) = 25$$
$$(g \circ f)((2,5)) = g(f((2,5)) = g(2-5) = g(-3) = -24$$

(ii) Behauptung: $(f \circ g)(2)$ kann nicht berechnet werden.

Beweis. Die Hintereinanderausführung $(f \circ g)$ ist nicht definiert, da die Wertemenge $\mathbb{R}$ von g nicht mit dem Definitionsbereich $\mathbb{R}\times\mathbb{R}$ von f übereinstimmt. □

Aufgabe 21

(a) Behauptung: $f : \mathbb{N} \to \mathbb{N}$, $n \mapsto n+5$ ist injektiv aber nicht surjektiv.

Beweis. Injektivität: Sind $n, n' \in \mathbb{N}$ mit $f(n) = f(n')$, so gilt $n+5 = n'+5$ und damit $n = n'$.
Surjektivität: $4 \in \mathbb{N}$ besitzt kein Urbild unter f. Annahme: Es gibt ein $n \in \mathbb{N}$ mit $f(n) = 4 = n+5$. Dann ist $n = -1 \in \mathbb{N}$. Dies ist aber ein Widerspruch, da $-1 \notin \mathbb{N}$. □

(b) Behauptung: $g : \mathbb{R}\times\mathbb{R} \to \mathbb{R}$, $(x,y) \mapsto x-y$ ist surjektiv aber nicht injektiv.

Beweis. Injektivität: Es sind $(2,1),(3,2) \in \mathbb{R}\times\mathbb{R}$ und $(2,1) \neq (3,2)$. Aber $g(2,1) = 2-1 = 1 = 3-2 = g(3,2)$. Damit ist g nicht injektiv.
Surjektivität: Sei $x \in \mathbb{R}$ beliebig, dann ist $(x,0) \in \mathbb{R}\times\mathbb{R}$ und $g(x,0) = x-0 = x$. Wir können also zu jedem $x \in \mathbb{R}$ ein Urbild finden. Damit ist g surjektiv. □

Übungsblatt 6

Aufgabe 22

Es sei $G \subseteq \mathbb{N}$ die Menge der geraden natürlichen Zahlen.

(a) Zu zeigen: $G \subset \mathbb{N}$. (Manchmal auch $G \subsetneq \mathbb{N}$ geschrieben)

Beweis. $G \subset \mathbb{N}$ heißt ja: $G \subseteq \mathbb{N}$ und $G \neq \mathbb{N}$. Wir haben $1 \in \mathbb{N}$, aber $1 \notin G$. Also kann nicht $\mathbb{N} = G$ gelten. □

(b) Zu zeigen: Die Abbildung $f : \mathbb{N} \longrightarrow G$, $n \longmapsto 2 \cdot n$ ist injektiv und surjektiv (und damit bijektiv).

Beweis. Injektivität: Wir wollen zeigen: $\forall n,n' \in \mathbb{N} : f(n) = f(n') \Longrightarrow n = n'$. Seien also $n,n' \in \mathbb{N}$ mit $f(n) = f(n')$ beliebig, dann ist $2 \cdot n = 2 \cdot n'$ und damit $n = n'$.
Surjektivität: Wir wollen zeigen $\forall n \in G \exists m \in \mathbb{N} : f(m) = n$. Sei also $n \in G$ beliebig. Dann hat n die Form $2 \cdot m$ mit einem $m \in \mathbb{N}$, da n gerade. Also ist $f(m) = 2 \cdot m = n$. □

(c) Gesucht ist die Umkehrabbildung $g : G \longrightarrow \mathbb{N}$ mit $f \circ g = \mathrm{id}_G$ und $g \circ f = \mathrm{id}_{\mathbb{N}}$.
Behauptung: $g : G \longrightarrow \mathbb{N}, n \longmapsto \frac{n}{2}$ ist die Umkehrabbildung.

Beweis. Zunächst sind alle $n \in G$ gerade und damit ist $\frac{n}{2} \in \mathbb{N}$ und es gelten:
$\forall n \in \mathbb{N} : (g \circ f)(n) = g(2n) = \frac{2n}{2} = n$ und
$\forall n \in G : (f \circ g)(n) = f(\frac{n}{2}) = 2 \cdot \frac{n}{2} = n$ und damit $f \circ g = \mathrm{id}_G$ und $g \circ f = \mathrm{id}_{\mathbb{N}}$. □

Aufgabe 23, CAESAR

Zunächst setzen wir $\mathcal{A} := \{\mathrm{A,B,C,D,\ldots,X,Y,Z}\}$ das Alphabet. Die Abbildung $\varphi : \mathcal{A} \longrightarrow \mathcal{A}$ ist definiert durch:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

(a) Wie sich aus obiger Tabelle ergibt: $\varphi(\mathrm{X}) = \mathrm{A}, \varphi(\mathrm{Y}) = \mathrm{B}, \varphi(\mathrm{Z}) = \mathrm{C}$.

(b) Wir wenden auf jeden Buchstaben der Worte VENI VIDI VICI die Abbildung φ an und erhalten: YHQLYLGLYLFL.

(c) Aus der obigen Definition von φ ist ersichtlich, daß jedes Element aus $\mathcal{A}$ *genau ein* Urbild unter φ hat. Also ist φ bijektiv. Die Entschlüsselungsfunktion φ^{-1} weist jedem Element von $\mathcal{A}$ sein Urbild unter φ zu:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

(d) Wende auf jeden Buchtaben des Geheimtextes “GDVLVWHLQIDFK” die Abbildung φ^{-1} an. Dann erhält man: DASISTEINFACH $\simeq$ DAS IST EINFACH.

Aufgabe 24

Es ist durch Induktion zu zeigen:

(a) Für $n \in \mathbb{N}$ bezeichne s_n die Summe aller ungeraden natürlichen Zahlen von 1 bis $2n-1$. Suche eine Formal für s_n in Abhängigkeit von n und beweise diese durch vollständige Induktion.
Beobachtung: $s_1 = 1,\ s_2 = 4,\ s_3 = 9,\ s_4 = 14, \ldots$
Behauptung: $s_n = n^2$.

Beweis. Induktionsanfang, $n = 1 : s_1 = 1 = 1^2$, also ist die Behauptung für $n = 1$ richtig.
Induktionsvoraussetzung: Die Formel gelte für eine bestimmte natürliche Zahl $n \in \mathbb{N}$, also $s_n = n^2$.
Induktionsbehauptung: $s_{n+1} = (n+1)^2$.
Induktionsschritt:

$$s_{n+1} = 1+3+5+\cdots+(2n-1)+(2n+1) = s_n + (2n+1)$$
$$\stackrel{\mathrm{IV}}{=} n^2 + (2n+1) = n^2 + 2n + 1 = (n+1)^2.$$

□

(b) Für $n \in \mathbb{N}$ sei $t_n := 1 \cdot 2 + 2 \cdot 3 + \cdots + n \cdot (n+1)$.
Zu zeigen: $\forall n \in \mathbb{N} : t_n = \frac{1}{3} n(n+1)(n+2)$.

Beweis. Induktionsanfang, $n=1: t_1 = 1(1+1) = 2 = \frac{1}{3}1(1+1)(1+2)$. Also ist die Behauptung für $n=1$ richtig.
Induktionsvoraussetzung: Die Formel gelte für eine bestimmte natürliche Zahl $n \in \mathbb{N}$, also $t_n = \frac{1}{3}n(n+1)(n+2)$.
Induktionsbehauptung: $t_{n+1} = \frac{1}{3}(n+1)(n+2)(n+3)$.
Induktionsschritt:

$$\begin{aligned} t_{n+1} &= 1\cdot 2 + 2\cdot 3 + \cdots + n(n+1) + (n+1)(n+2) = t_n + (n+1)(n+2) \\ &\overset{\text{IV}}{=} \frac{1}{3}n(n+1)(n+2) + (n+1)(n+2) = (\frac{1}{3}n+1)((n+1)(n+2)) \\ &= \frac{1}{3}(n+3)(n+1)(n+2) = \frac{1}{3}(n+1)(n+2)(n+3). \end{aligned}$$

□

Übungsblatt 7

Aufgabe 25

Die *Alle Autos haben die gleiche Farbe*-Aufgabe.
Wir setzen $P(n) :\Longleftrightarrow$ je n Autos haben die gleiche Farbe. Um die Behauptung der Aufgabenstellung zu zeigen, müßte ein Induktionsbeweis folgendermaßen vorgehen:
Induktionsanfang: $P(1)$, also ein Auto hat die gleich Farbe wie es selbst.
Induktionsschluß: $\forall n \in \mathbb{N}: P(n) \Longrightarrow P(n+1)$, aber die Argumentation aus der Aufgabenstellung versagt für den Fall $n=2$, da es zwei Autos mit verschiedenen Farben gibt.

Aufgabe 26

Gesucht ist eine Rekursionsgleichung für

$$a_n := \left|\left\{x \,\middle|\, x \in \{0,1\}^n, \text{ in } x \text{ kommen keine aufeinanderfolgenden Nullen vor}\right\}\right|.$$

Bis $n=5$ geben wir die Zahlen explizit an:
$n=1$: $1, 0$, also $a_1 = 2$.
$n=2$: $01, 10, 11$, also $a_2 = 3$.
$n=3$: $010, 110, 011, 101, 111$, also $a_3 = 5 = 2+3$.
$n=4$: $0110, 1010, 1110, 0101, 1101, 0111, 1011, 1111$, also $a_4 = 8 = 5+3$.
$n=5$: $01101, 10101, 11101, 01011, 11011, 01111, 10111, 11111, 01010, 11010, 01110,$
$10110, 11110$, also $a_5 = 13 = 8+5$
So kommen wir zu dem Verdacht: $\forall n \geq 3: a_n = a_{n-1} + a_{n-2}$, den wir beweisen wollen. Dazu definieren wir zunächst:
Eine n-Folge $x \in \{0,1\}^n$ heißt *zulässig,* wenn keine aufeinanderfolgenden Glieder Null sind.

Beweis. Jede n-Folge $x \in \{0,1\}^n$ endet entweder mit Null oder mit Eins. Wir haben also zwei Fälle:
1. Fall: Folge endet mit 1, Dann bilden die Glieder davor eine zulässige $(n-1)$-Folge, davon gibt es a_{n-1} viele.
2. Fall: Folge endet mit 0, dann darf die Stelle davor nicht 0 sein, also endet die Folge auf 10. Die Glieder davor müssen eine zulässige $(n-2)$-Folge sein, davon gibt es a_{n-2} viele. □

Damit haben wir die Rekursionsgleichung

$$a_1 = 2,\ a_2 = 3,\ a_{n+2} = a_{n+1} + a_n \qquad \text{für alle } n \in \mathbb{N}$$

bewiesen. Diese Gleichung entspricht der der FIBONACCI-Zahlen mit den Anfangswerten $F_3 = a_1 = 2,\ F_4 = a_2 = 3$ und damit $a_n = F_{n+2}$.

Aufgabe 27

Die Zahlen b_n, $n \in \mathbb{N}$ seien rekursiv definiert durch $b_0 := 1$, $b_1 := 2$, $b_n := 2b_{n-1} - b_{n-2}$ für $n \geq 2$.
Die ersten sieben Zahlen sind:

$b_0 = 1,\ b_1 = 2,\ b_2 = 3,\ b_3 = 4,\ b_4 = 5,\ b_5 = 6,\ b_6 = 7,\ b_7 = 8.$

Gesucht ist jetzt eine Formel für die b_n. Unsere Vermutung ist: $b_n = n+1$ für $n \geq 2$.

Beweis. Induktionsanfang: $n = 2$: $b_2 = 3 = 2+1$ und $n = 3$: $b_3 = 4 = 3+1$.
Induktionsvoraussetzung: Sei $n \geq 4$ beliebig und die Behauptung richtig für $n-1$ und $n-2$, also

$b_{n-1} = n$ und $b_{n-2} = n-1$.

Induktionsbehauptung: $b_n = n+1$.
Induktionsschluß: $b_n \overset{\text{Def.}}{=} 2b_{n-1} - b_{n-2} \overset{\text{(IV)}}{=} 2(n) - (n-1) = 2n - n + 1 = n+1$. □

Beachte: Da $b_4 = 2b_3 - b_2$ muß der Induktionsanfang für $n = 2$ und $n = 3$ geführt werden. Im Induktionsschluß zeigt man dann "$P(n-1) \wedge P(n-2) \Longrightarrow P(n)$."

Aufgabe 28 (Türme von Hanoi)

Zunächst vereinbaren wir die Schreibweise $A \xrightarrow{k} B$ für: Die k-te Scheibe wird von A nach B gelegt.
Das Spiel mit einer Scheibe braucht trivialerweise genau einen Zug.

(1) Wir spielen jetzt mit zwei Scheiben: $A \xrightarrow{1} B,\ A \xrightarrow{2} C,\ B \xrightarrow{1} C$ und brauchen drei Züge.

(2) Mit drei Scheiben: $A \xrightarrow{1} C,\ A \xrightarrow{2} B,\ C \xrightarrow{1} B,\ A \xrightarrow{3} C,\ B \xrightarrow{1} A,\ B \xrightarrow{2} C,\ A \xrightarrow{1} C$ und brauchen sieben Züge.

(3) Nach dem dritten Zug haben wir die Situation, eine Scheibe nach Säule C verlagern zu müssen, sowie das Spiel mit zwei Scheiben von B nach C. In den ersten Drei Schritten haben wir das Spiel mit zwei Scheiben von A nach B gespielt.

(4) Wir wissen $s_1 = 1$ und vermuten $s_n = 2s_{n-1} + 1$ für $n \geq 2$.

Beweis. Induktionsanfang: $s_2 = 3 = 2 \cdot 1 + 1 = 2 \cdot s_1 + 1$.
Induktionsvoraussetzung: Für ein beliebiges $n \geq 2$ gelte $s_n = 2s_{n-1} + 1$.
Induktionbehauptung: $s_{n+1} = 2s_n + 1$
Induktionsschritt: Wir spielen das Spiel mit $n+1$ Scheiben. Die oberen n Scheiben lassen sich nach Induktionsvoraussetzung in s_n Zügen von A nach B legen. Dann wird die $n+1$te Scheibe nach C gelegt, und in weiten s_n Zügen der Stapel mit n Scheiben von B nach C. Insgesamt erhalten wir so $s_{n+1} = s_n + 1 + s_n = 2 \cdot s_n + 1$ Züge. □

(5) Gesucht ist eine *geschlossene Formel* für s_n, also eine Formel, die nich nicht auf s_{n-1} abstützt. Dazu berechnen wir zunächst einige s_n explizit:

$s_1 = 1 = 2-1 = 2^1 - 1, \quad s_2 = 3 = 4-1 = 2^2 - 1,$
$s_3 = 7 = 8-1 = 2^3 - 1, \quad s_4 = 15 = 16-1 = 2^4 - 1, \ \ldots$

und gelangen so zu der Vermutung $s_n = 2^n - 1$ für alle $n \geq 1$.

Beweis. Induktionsanfang s.o.
Induktionsvoraussetzung: Für ein $\mathbb{N} \ni n \geq 2$ gelte $s_n = 2^n - 1$.
Induktionsbehauptung: $s_{n+1} = 2^{n+1} - 1$.
Induktionsschritt: $s_{n+1} = 2 \cdot s_n + 1 \overset{\text{IV}}{=} 2 \cdot (2^{n-1} - 1) + 1 = 2 \cdot 2^{n-1} - 2 + 1 = 2^n - 1$ □

Übungsblatt 8

Aufgabe 29

(a) Zu berechnen: $\sum_{k=0}^{5} k\binom{5}{k}$

$$\sum_{k=0}^{5} k\binom{5}{k} = 0\binom{5}{0} + 1\binom{5}{1} + 2\binom{5}{2} + 3\binom{5}{3} + 4\binom{5}{4} + 5\binom{5}{5}$$

$$\text{mit } 1 = \binom{5}{5} = \binom{5}{0}, \quad 5 = \binom{5}{1} = \binom{5}{5-1} = \binom{5}{4}, \quad 10 = \binom{5}{2} = \binom{5}{3}$$

$$= 0 \cdot 1 + 1 \cdot 5 + 2 \cdot 10 + 3 \cdot 10 + 4 \cdot 5 + 5 \cdot 1$$

$$= 80$$

(b) Gesucht ist der Koeffizient von x^{14} in dem Ausdruck $(1-2x^2)^{10}$.
Nach dem binomischen Satz (7.11) gilt

$$(1-2x^2)^{10} = \sum_{k=0}^{10} \binom{10}{k} 1^{10-k}(-2x^2)^k = \sum_{k=0}^{10} \binom{10}{k}(-2x^2)^k.$$

Den gesuchten Koeffizienten enthält man demzufolge für $k = 7$:

$$\binom{10}{7}(-2)^7 = -\binom{10}{7}2^7 = -\binom{10}{3}2^7 = -\frac{10 \cdot 9 \cdot 8}{1 \cdot 2 \cdot 3} \cdot 2^7 = -120 \cdot 2^7 = -15360$$

Aufgabe 30

(a) Zu berechnen: $\sum_{k=0}^{n}(-1)^k\binom{n}{k}$ für $n \in \mathbb{N}_0$.
Nach bem binomischen Lehrsatz ist $(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k$ für alle $x, y \in \mathbb{R}$ und $n \in \mathbb{N}_0$. Setze nun $x := 1$, $y := -1$, und erhalte

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k} = \sum_{k=0}^{n}\binom{n}{k}1^{n-k}(-1)^k = (1+(-1))^n = 0^n$$

$$= \begin{cases} 1 & \text{für } n = 0 \\ 0 & \text{für } n \geq 1 \end{cases}.$$

(b) Sei M eine endliche Menge mit $n \geq 1$ Elementen. Setze

$g_n :=$ Anzahl der Teilmengen von M, die gerade Elementzahl haben,

$u_n :=$ Anzahl der Teilmengen von M, die ungerade Elementzahl haben.

Zu zeigen: $g_n = u_n$.

Beweis. Nach Satz (7.9) ist $\binom{n}{k}$ die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge, d.h.

$$g_n = \sum_{k=0, k \text{ gerade}}^{n} \binom{n}{k},$$

$$u_n = \sum_{k=0, k \text{ ungerade}}^{n} \binom{n}{k}.$$

Weiterhin gilt $(-1)^k = \begin{cases} 1 & k \text{ gerade} \\ -1 & k \text{ ungerade} \end{cases}$.

Aus (a) folgt für $n \geq 1$:

$$0 = \sum_{k=0}^{n} (-1)^k \binom{n}{k} = \sum_{k=0, k \text{ gerade}}^{n} \binom{n}{k} + \sum_{k=0, k \text{ ungerade}}^{n} (-1) \binom{n}{k}$$
$$= \sum_{k=0, k \text{ gerade}}^{n} \binom{n}{k} - \sum_{k=0, k \text{ ungerade}}^{n} \binom{n}{k} = g_n - u_n$$

Daraus folgt $g_n = u_n$. □

Aufgabe 31

Sei M eine endliche Menge mit n Elementen, $M = \{x_1, \ldots, x_n\}$. Gesucht ist die Anzahl z_n der Möglichkeiten, M als disjunkte Vereinigung zweier nichtleerer Teilmengen darzustellen.
Für 2, 3 und 4 geben wir die Möglichkeiten explizit an:
$n = 2$: $\{\{x_1\}, \{x_2\}\}$, also $z_2 = 1$.
$n = 3$: $\{\{x_1, x_2\}, \{x_3\}\}$, $\{\{x_2, x_3\}, \{x_1\}\}$, $\{\{x_1, x_3\}, \{x_2\}\}$, also $z_3 = 3$.
$n = 4$: Eine 2-Zerlegung von M kann aus einer ein- und einer dreielementigen Teilmenge oder aus zwei zweielementigen Teimengen bestehen: Mit paarweise verschiedenen $i, j, k, l \in \{1, 2, 3, 4\}$ gibt es für

$\{\{x_i\}, \{x_j, x_k, x_l\}\}$ vier Möglichkeiten und für

$\{\{x_i, x_j\}, \{x_k, x_l\}\}$ drei Möglichkeiten, denn $\{\{x_i, x_j\}, \{x_k, x_l\}\} = \{\{x_k, x_l\}, \{x_i, x_j\}\}$

und damit ist $z_4 = 7$.
Sei nun $n \geq 2$ beliebig, gesucht ist die Anzahl der Zerlegungen von M, also die Anzahl der Mengen

$$\{U, V\},\ U, V \subseteq M, \text{ mit } U \neq \emptyset \wedge V \neq \emptyset \wedge U \cup V = M \wedge U \cap V = \emptyset.$$

Daraus folgt $V = M \backslash U$.
Da U, V beide nichtleer und damit ungleich M sein müssen, gibt es für U insgesamt $2^n - 2$ Möglichkeiten. Wegen $M \backslash (M \backslash U) = U$ liefern aber U und $M \backslash U = V$ dieselben Zerlegungen, d.h.

$$z_n = \frac{1}{2}(2^n - 1) = 2^{n-1} - 1 \quad \text{für alle } n \geq 1.$$

Aufgabe 32

Es sei M eine endliche Menge und $T \subseteq M$ eine Teilmenge von M.

(a) Zu zeigen: Aus $|T| = |M|$ folgt $T = M$.

Beweis. $M = T \cup (M \backslash T) \Longrightarrow [(7.4b)]\ |M| = |T| + |M \backslash T| \Longrightarrow [|T| = |M| \text{ n.V.}]\ |M \backslash T| = 0$ und damit ist $M \backslash T = \emptyset$, also liegt jedes Element aus M auch in T, d.h. $M \subseteq T$. Nach Voraussetzung ist aber auch $T \subseteq M$ und damit $T = M$. □

(b) Die Voraussetzung, daß M endlich sein muß, ist nicht verzichtbar, denn $\mathbb{N} \subseteq \mathbb{Z}$, $|\mathbb{N}| = |\mathbb{Z}|$ aber $\mathbb{Z} \ni -1 \notin \mathbb{N}$, also $\mathbb{N} \neq \mathbb{Z}$.

(c) Es seien M, N Mengen und $f : M \to N$ eine injektive Abbildung. Zu zeigen: $|f(M)| = |M|$. (Das gilt auch wenn M nicht endlich ist.)

Beweis. f definiert eine bijektive Abbildung $g : M \to f(M), x \mapsto f(x)$. Da f injektiv ist, ist auch g injektiv, nach Definition von $f(M)$ ist g auch surjektiv, also ist g bijektiv. Also $M \sim f(M)$ und somit $|M| = |f(M)|$. (Hier wird nirgendwo benutzt, daß M endlich ist.) □

(d) Seien M, N endliche Mengen mit $|M| = |N|$. Zu zeigen: jede injektive Abbildung $f : M \to N$ ist bijektiv.

Beweis. Zu zeigen ist, daß f surjektiv ist, also $f(M) = N$. Es gilt $f(M) \subseteq N$ mit $|f(M)| \overset{(c)}{=} |M| \overset{\text{Vor.}}{=} |N|$. Nach (a) folgt $f(M) = N$. □

(e) Die Eigenschaft der Endlichkeit von N und M ist nicht verzichtbar, denn $f : \mathbb{N} \to \mathbb{N}$, $n \mapsto n+5$ ist injektiv aber nicht surjektiv (siehe Übungsaufgabe 21a) und $|\mathbb{N}| = \infty$.

Übungsblatt ⋆9⋆

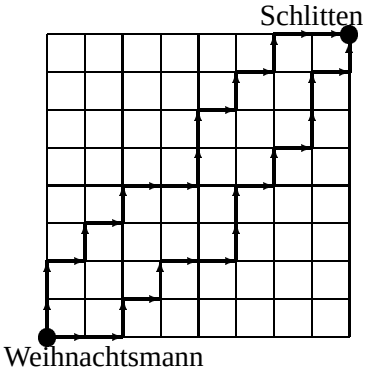
Aufgabe 33 (Weihnachtsmann)

(a) Wieviele Möglichkeiten hat der Weihnachtsmann, einem *lieben* Studenten vier Geschenke aus einer Liste von 30 zu schenken?
Gesucht ist die Anzahl der vierelementigen Teilmengen einer 30-elementigen Menge, wir müssen das *Lotto-Problem* lösen. Es gibt also $\binom{30}{4}$ Möglichkeiten.

(b) Wieviele Möglichkeiten hat der Weihnachtsmann, seine acht Rentiere anzuspannen, wenn *der rotnasige Rudi* immer vorne rechts stehen soll?
Da Rudis Position immer vorgegeben ist, kann der Weihnachtsmann nur noch die Positionen der anderen sieben Rentiere variieren. Er hat also sieben Plätze und sieben Rentiere, und damit 7! Möglichkeiten.

(c) Der Weihnachtsmann besucht 30 Studenten, und gibt jedem fleißigen Studenten ein Geschenk, jedem faulen keins. Wieviele Geschenkverteilszenarien sind denkbar?
Wir kodieren faule Studenten kanonisch als “0”, fleißige als “1”. Damit wird jedes Szenario eindeutig durch eine 30-stellige Binärfolge dargestellt. Hiervon gibt es genau 2^{30} Stück.

(d) Wieviele kürzeste Wege gibt es vom Weihnachtsmann zum Schlitten?
Wir sehen uns zunächst einige kürzeste Wege an:



Der Weihnachtsmann kann jedesmal ein Straßenstück nach oben (O) oder nach rechts (R) bis zur nächsten Kreuzung gehen. Bewegungen nach links oder unten sind nicht möglich, denn sie würden einen Umweg bedeuten. Auf jedem kürzesten Weg geht er also acht mal nach rechts und acht mal nach oben.
Jeder solche Weg ist durch ein 16 Zeichen langes Wort aus acht mal O und acht mal R eindeutig beschrieben. Nach Satz (8.4) gibt es hiervon gerade

$$\binom{16}{8,\ 8} = \frac{16!}{8! \cdot 8!} = \frac{16!}{8! \cdot (16-8)!} = \binom{16}{8} = 12870$$

viele.

(e) Wieviele Möglichkeiten hat Kevins Schwester, sich zehn Leckereien von einem Teller mit jeweils mindestens zehn Mandarinen, Nüssen und Plätzchen zu nehmen?

Es werden zehn Teile auf die drei Kästen M (Mandarinen), N (Nüsse) und P (Plätzchen) verteilt, d.h. es handelt sich um eine Kombination mit Wiederholung ohne Berücksichtigung der Reihenfolge. Nach Satz (8.13) ist deren Anzahl

$$C_W(3,10) = \binom{3-1+10}{10} = \binom{12}{10} = \binom{12}{2} = 66.$$

Aufgabe 34

Auf der Menge $\mathcal{A} = \{a,b,c,\ldots,y,z\}$ der Buchstaben des Alphabets ist durch die übliche Reihenfolge der Buchstaben eine linerae Ordnung $\preceq$ definiert (z.B. gilt $a \preceq a,\ c \preceq r$ aber $y \not\preceq n$). Wir nennen ein Wort $w = w_1 w_2 \ldots w_k$ aus den Buchstaben $w_1,\ldots,w_k \in \mathcal{A}$ *monoton steigend*, wenn gilt: $\forall i,j \in \{1,2,\ldots k\} : i < j. \Longrightarrow w_i \preceq w_j$. Es bezeichne a_k die Anzahl der monoton steigenden Wörter der Länge k

(a) Gesucht ist a_k für $k = 1,2,3$ jeweils durch explizite Überlegung.
Für $k = 1$ ist klar, daß jedes Wort der Länge eins monoton steigend ist, es gilt also $a_k = 26$.
Für $k = 2$ bilden wir alle monoton steigenden Wörter, nach Anfangsbuchstaben sortiert:

$$\begin{array}{rl} aa,\ ab,\ ac,\ \ldots,az & 26 \\ bb,\ bc,\ \ldots,bz & 25 \\ cc,\ \ldots,cz & 24 \\ \ddots & \vdots \\ yy,\ yz & 2 \\ zz & 1 \end{array}$$

Wir haben also $a_2 = 26+25+\ldots+2+1 = \sum_{i=1}^{26} i = \frac{26\cdot 27}{2}$.
Für $k = 3$ erhalten wir die Tabelle

$$\begin{array}{rl} aaa,\ aab,\ aac,\ \ldots,azz & \frac{26\cdot 27}{2} \\ bbb,\ bbc,\ \ldots,bzz & \frac{25\cdot 26}{2} \\ ccc,\ \ldots,czz & \frac{24\cdot 25}{2} \\ \ddots & \vdots \\ zzz & 1 \end{array}$$

Monoton steigende Wörter der Länge drei mit Anfangsbuchstaben a gibt es genau a_2 viele, mit Anfangsbuchstaben b genau so viele, wie es monoton steigende Wörter der Länge zwei aus den Buchstaben $b,c,\ldots,z$ gibt usw.
Damit erhalten wir: $a_3 = \sum_{i=1}^{26} \frac{i(i+1)}{2} = \frac{1}{2}\sum_{i=1}^{26} i(i+1) \overset{\text{Aufg. 24b}}{=} \frac{26\cdot 27\cdot 28}{2\cdot 3}$.

(b) Gesucht ist eine allgemeine Formel für a_k für beliebige $k \in \mathbb{N}$.
Da es bei einer k-Multimenge nicht auf die Reihenfolge der Elemente ankommt, wird jede k-Multimenge, die aus den Buchstaben von $\mathcal{A}$ gebildet werden kann, durch ein eindeutig bestimmtes, monoton steigendes Wort beschrieben. Also ist die Anzahl a_k der monoton steigenden Wörter aus k Buchstaben vob $\mathcal{A}$ gleich der Anzahl der k-Multimengen aus 26 Elementen. Folglich ist nach (8.13):

$$a_k = C_W(26,k) = \binom{26-1+k}{k} = \binom{25+k}{k}.$$

Für $k = 1,2,3$ erhalten wir in Übereinstimmung mit (a):

$$a_1 = \binom{25+1}{1} = \binom{26}{1} = 26$$
$$a_2 = \binom{25+2}{2} = \binom{27}{2} = \frac{26\cdot 27}{2}$$
$$a_3 = \binom{25+3}{3} = \binom{28}{3} = \frac{26\cdot 27\cdot 28}{2\cdot 3}.$$

Übungsblatt 10

Aufgabe 35

Gesucht ist die Wahrscheinlickkeit, daß ein zufälliges Paar $(a,b) \in \{1,\ldots,10\}\times\{1,\ldots,10\}$ aus zwei teilerfremden Zahlen a,b besteht.
Zunächst definieren wir

$$M := \{1,\ldots,10\}\times\{1,\ldots,10\},$$
$$N := \big\{(a,b)\big|\ (a,b)\in M,\ \mathrm{ggT}(a,b)=1\big\}.$$

Die gesuchte Wahrscheinlichkeit ist dann $W = \frac{|N|}{|M|}$.
Um die Mächtigkeit von N zu bestimmen, berechnen wir folgende Werte für $a = 1,\ldots,10$:

$$s_a = \big|\big\{x\big|\ x\in\{1,\ldots,10\},\ \mathrm{ggT}(a,x)=1\big\}\big|.$$

indem wir die Mengen einfach abzählen und erhalten:

$$s_1 = 10 \quad s_2 = 5 \quad s_3 = 7 \quad s_4 = 5 \quad s_5 = 8$$
$$s_6 = 3 \quad s_7 = 9 \quad s_8 = 5 \quad s_9 = 7 \quad s_{10} = 4$$

Nun ist $|N| = a_1 + a_2 + \ldots + a_{10} = 63$ und die gesuchte Wahrscheinlichkeit

$$W = \frac{|N|}{|M|} = \frac{63}{100} = 0.63 = 63\%.$$

Aufgabe 36

Ein Bauer im Lippischen[1] besitzt einen rechteckigen Acker. Dieser ist 143 Meter lang und 77 Meter breit. Besagter Bauer will diesen Acker rundherum einzäunen. Dazu will er so wenig Pfähle wie möglich verwenden. Alle Pfähle sollen denselben Abstand zueinander haben; hierbei sind nur ganze Meter als Abstand zulässig! Aus Stabilitätsgründen muss an jeder Ecke ein Pfahl eingeschlagen werden. Wieviele Pfähle braucht der Bauer mindestens?

Sei a der Abstand zweier aufeinanderfolgender Pfähle. Nach Aufgabenstellung muß $a \in \mathbb{N}$ gelten. Da die Pfähle alle gleichen Abstand haben, muß gelten

$$\left.\begin{array}{l} a\cdot s = 77 \\ a\cdot t = 143 \end{array}\right\} \Longrightarrow a\big|77 \wedge a\big|143,$$

da a maximal sein soll, muß also $a = \mathrm{ggT}(77,143)$ gelten.
Wir benutzen den *Euklidischen Algorithmus,* um den ggT zu berechnen:

$$\begin{aligned} 143 &= 1\cdot 77 + 66 \\ 77 &= 1\cdot 66 + 11 \\ 66 &= 6\cdot 11 + 0 \qquad \Longrightarrow 11 = \mathrm{ggT}(143,77). \end{aligned}$$

Nun berechnen wir noch $s = \frac{77}{a} = \frac{77}{11} = 7$ und $t = \frac{143}{a} = \frac{143}{11} = 13$. Die Gesamtzahl der benötigten Pfosten ist also $2\cdot s + 2\cdot t = 40$.

[1] Die Fragestellung ist auch ohne die Voraussetzung *im Lippischen* möglich.

Aufgabe 37 (RSA)

(1) Warum sind $p = 37$ und $q = 29$ Primzahlen?
Durch testen aller Primzahlen kleiner als $\lfloor\sqrt{p}\rfloor$ bzw. $\lfloor\sqrt{q}\rfloor$ liefert, daß p, q keine echten Teiler haben.

(2) $N = p \cdot q = 37 \cdot 29 = 1073$ und $M = (p-1)\cdot(q-1) = 36 \cdot 29 = 1008$.

(3&4) Wähle $e = 275$ zufällig mit $1 < e < M = 1008$, gesucht ist nun $e^{-1} \pmod M$, dieses wird mit dem *Erweiterten Euklidischen Algorithmus* berechnet, mit dem wir auch $\mathrm{ggT}(e, M) = 1$ überprüfen.

$$1008 = 3 \cdot 275 + 183$$
$$275 = 1 \cdot 183 + 92$$
$$183 = 1 \cdot 92 + 91$$
$$92 = 1 \cdot 91 + \boxed{1}$$
$$91 = 91 \cdot 1 + 0$$
$$\Longrightarrow \mathrm{ggT}(1008, 275) = 1$$

k	0	1	2	3	4	5	6
r_k	1008	275	183	92	91	1	0
q_k	—	3	1	1	1	91	
x_k	1	0	1	-1	2	-3	
y_k	0	1	-3	4	-7	11	

$$\Longrightarrow 1 = (-3)\cdot 1008 + 11 \cdot 275$$
$$\Longrightarrow 11 \cdot 275 \equiv 1 \pmod{1008}$$

So setzen wir $d := 11$ und erhalten (e, N) als öffentlichen und (d, N) als privaten Schlüssel.

(5) Jetzt soll die verschlüsselte Nachricht $y = 1006$ entschlüsselt werden: Wir wissen $y \equiv m^{275} mod N$, wobei m die geheime Nachricht ist. Zur Entschlüsselung berechnen wir $m = y^d = 1006^{11} \pmod{1008}$. Dies liefert $m = 123$.
Bemerkung: Um 1006^{11} zu berechnen, benutzen wir die Methode des *sukzessiven Quadrierens:*

$$1006^2 = 1012036 \pmod N = 197$$
$$1006^4 = 197^2 = 38809 \pmod N = 181$$
$$1006^8 = 181^2 = 32761 \pmod N = 571$$
$$1006^{10} = 571 \cdot 197 = 112487 \pmod N = 895$$
$$1006^{11} = 895 \cdot 1006 = 900370 \pmod N = 123$$

Aufgabe 38

Wandle die Dezimalzahlen $a = 141$ und $b = 152$ in Zahlen zur Basis 4 um, addiere und multipliziere diese Zahlen in der Darstellung zur Basis 4 und überprüfe die Ergebnisse, indem du sie wieder in Dezimalzahlen umwandelst und mit den Dezimalzahlen $a + b$ bzw. $a \cdot b$ vergleichst.
Zunächst bestimmen wir also nun die Darstellung von a und b zur Basis 4:

$$141 = 35 \cdot 4 + 1 \qquad 152 = 38 \cdot 4 + 0$$
$$35 = 8 \cdot 4 + 3 \qquad 38 = 9 \cdot 4 + 2$$
$$8 = 2 \cdot 4 + 0 \qquad 9 = 2 \cdot 4 + 1$$
$$2 = 0 \cdot 4 + 2 \qquad 2 = 0 \cdot 4 + 2$$
$$\Longrightarrow a = (2031)_4 \qquad \Longrightarrow b = (2120)_4$$

Nun berechnen wir Summe und Produkt:

$$\begin{array}{rr} & (2031)_4 \\ + & (2120)_4 \\ \hline & (10211)_4 \end{array} \qquad \begin{array}{rr} & (2031)_4 \cdot (2120)_4 \\ \hline & (101220)_4 \\ & (2031\ \ )_4 \\ & (10122\ \ \ )_4 \\ \hline & (11032320)_4 \end{array}$$

Die Ergebnisse rechnen wir nun mit Hilfe des *Horner-Schemas* in die Dezimaldarstellung um:

	1	0	2	1	1
4	—	4	16	72	292
	1	4	18	73	$\boxed{293}$

	1	1	0	3	2	3	2	0
4	—	4	20	80	332	1336	5356	21432
	1	5	20	83	334	1339	5358	$\boxed{21432}$

Also ist $(10211)_4 = 293 = 141 + 152$, $(11032320)_4 = 21432 = 141 \cdot 152$ und unsere Rechnungen waren korrekt.

Übungsblatt 11

Aufgabe 39

(a) Zu zeigen: Jede natürlich Zahl $n \in \mathbb{N}$, die weder von 2 noch von 3 geteilt wird. läßt sich n in der Form $n = 6k+1$ oder $n = 6k-1$ mit einem geeigneten $k \in \mathbb{N}$ darstellen.

Beweis. Teilt man n mit Rest r durch 6, also $n = k \cdot 6 + r$ so gilt $r \in \{0, \ldots, 5\}$. Wir betrachten nun die folgenden Fälle:
$r = 0 \Longrightarrow n = 6 \cdot k \Longrightarrow 2 \mid n \wedge 3 \mid n$, Widerspruch zur Voraussetzung.
$r = 2 \Longrightarrow n = 6 \cdot k + 2 = 2(3 \cdot k + 1) \Longrightarrow 2 \mid n$, Widerspruch zur Voraussetzung.
$r = 3 \Longrightarrow n = 6 \cdot k + 3 = 3(2 \cdot k + 1) \Longrightarrow 3 \mid n$, Widerspruch zur Voraussetzung.
$r = 4 \Longrightarrow n = 6 \cdot k + 4 = 2(3 \cdot k + 2) \Longrightarrow 2 \mid n$, Widerspruch zur Voraussetzung.
Also können nur 1 und 5 als Reste auftreten, es gilt mit geeignetem $k \in \mathbb{N}_0$:
$r = 1 \Longrightarrow n = 6 \cdot k + 1$ bzw. $r = 5 \Longrightarrow n = 6 \cdot k + 5 = n = 6(k+1) + 1$. □

(b) Zu zeigen: Ist p eine Primzahl, so ist $p \equiv \pm 1 \pmod 6$.

Beweis durch Kontraposition. Ist $p \not\equiv \pm 1 \pmod 6$, so folgt nach (a), daß $3 \mid p$ oder $2 \mid p$, also ist p keine Primzahl. □

(c) Gesucht ist ein $k \in \mathbb{N}$ für das $6k+1$ und $6k-1$ keine Primzahlen sind.
Für $k = 20$ gilt $2k - 1 = 119 = 7 \cdot 17$ und $2k + 1 = 121 = 11 \cdot 11$. Wir sehen also, daß die Umhkehrung von (b) nicht gilt.

Aufgabe 40

Betrachte den folgenden Algorithmus für ungerade $n \in \mathbb{N}$:

```
1. x ← ⌊√n⌋
2. while (√(x²−n) ist kein Quadrat in ℕ) do
3.     x ← x+1
4. Antworte "x ± √(x²−n) sind zueinander komplementäre Teiler von n"
```

(a) Warum werden in `2.` wirklich Teiler von n gefunden?
Ist $\sqrt{x^2-n} \in \mathbb{N}_0$, so sind auch $x + \sqrt{x^2-n}$, $x - \sqrt{x^2-n} \in \mathbb{N}_0$. Bilden wir nun das Produkt, so erhalten wir

$$(x - \sqrt{x^2-n}) \cdot (x + \sqrt{x^2-n}) = x^2 - (\sqrt{x^2-n})^2 = x^2 - (x^2 - n) = n.$$

(b) Warum bricht das Verfahren spätestens bei $x = \frac{n+1}{2}$ ab?
Da n nach Voraussetzung ungerade sein soll, ist $n+1$ gerade und $\frac{n+1}{2} \in \mathbb{N}$. Ist $x = \frac{n+1}{2}$, so gilt

$$x^2 - n = \left(\frac{n+1}{2}\right)^2 - n = \frac{1}{4}(n^2+2n+1) - n = \frac{1}{4}(n^2+2n+1-4n)$$
$$= \frac{1}{4}(n^2-2n+1) = \frac{1}{4}(n-1)^2 = \left(\frac{n-1}{2}\right)^2, \text{ Quadratzahl}$$

Also bricht das Verfahren spätestens bei $x = \frac{n+1}{2}$ ab.

(c) Was bedeutet es für n, wenn das Verfahren erst für $x = \frac{n+1}{2}$ abbricht?
Nach (b) gilt dann

$$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2 = \left(\frac{n+1}{2} - \frac{n-1}{2}\right) \cdot \left(\frac{n+1}{2} + \frac{n-1}{2}\right)$$
$$= \frac{n+1-n+1}{2} \cdot \frac{n+1+n-1}{2} = \frac{2}{2} \cdot \frac{2n}{2} = 1 \cdot n$$

Es kann also keine Teiler außer 1 und n geben, da diese vorher gefunden worden wären, ist also $n \geq 3$, so ist n eine Primzahl.

(d) Es ist ein Teiler von $n := 96133$ zu berechnen:
Wir haben also $x = \lfloor\sqrt{96133}\rfloor = 310$ und führen den Algorithmus durch:

x	x^2-n	Quadrat?
310	-33	–
311	588	–
312	1211	–
313	1836	–
314	2463	–
315	3092	–
316	3723	–
317	4356	66^2

Also $x^2 - n = 66^2$. Damit haben wir

$$n = x^2 - 66^2 = (x-66)(x+66) = (317-66)(317+66) = 251 \cdot 383.$$

Aufgabe 41

Sei $p \in \mathbb{N}$ eine Primzahl. Zu zeigen: $\forall k \in \{1,\ldots,p-1\} : p \Big| \binom{p}{k}$.

Beweis. Wir haben $\binom{p}{k} = \frac{p!}{k!(p-k)!} \Longrightarrow \binom{p}{k} k!(p-k)! = p! = p \cdot (p-1)!$. D.h. p teilt den Ausdruck $\binom{p}{k} \cdot k! \cdot (p-k)!$. Da p prim ist, teilt nach (9.27b) p also mindenstens einen der drei Faktoren. Also $p \Big| \binom{p}{k} \vee p \Big| k! \vee p \Big| (p-k)!$.
Wir nehman an $p \Big| k!$, dann haben wir wieder nach (9.27b) $p \Big| 1 \cdot 2 \cdots k$, und p teilt ein $l \in \{1,\ldots,k\}$. Damit $p \leq l \leq k < p$, was ein Widerspruch ist.
Nun nehmen wir an $p \Big| (p-k)!$, dann teilt p nach (9.27b) ein $l \in \{1,\ldots,p-k\}$. Damit $p \leq l \leq (p-k) \leq (p-1)$, was ein Widerspruch ist.
Da die letzten beiden Fälle unmöglich sind, folgt die Behauptung $p \Big| \binom{p}{k}$. □

Aufgabe 42

Für die natürliche Zahl n haben wir die Darstellung $n = (a_r a_{r-1} \ldots a_1 a_0)_7$ mit $a_k \in \{0,1,\ldots,6\}\ \forall k$ bzüglich der Basis 7, also

$$n = a_r 7^r + a_{r-1} 7^{r-1} + \ldots + a_1 7 + a_0.$$

Weiter bezeichne $Q_7(n) := \sum_{k=0}^{r} a_k$ die Quersumme und $Q_7^{alt}(n) := \sum_{k=0}^{r}(-1)^k a_k$ die alternierende Quersumme von n.

(a) Zu zeigen: *(i)* $Q_7(n) \equiv n \pmod 3$,
(ii) $Q_7^{alt}(n) \equiv n \pmod 4$.

Beweis. *(i)* Aus $7 \equiv 1 \pmod 3$ folgt nach (9.37c) $\forall k \in \mathbb{N} : 7^k \equiv 1 \pmod 3$. Nach (9.37b) folgt dann $\forall k \in \{0,1,\ldots,r\} : a_k 7^k \equiv a_k \pmod 3$ und damit ist

$$n \equiv \sum_{k=0}^{r} a_k 7^k \equiv \sum_{k=0}^{r} a_k \equiv Q_7(n) \pmod 3.$$

(ii) Wir wissen $7 \equiv -1 \pmod 4$, daraus folgt nach (9.37c) $7^k \equiv (-1)^k \pmod 4$ für alle $k \in \mathbb{N}_0$. Wie in *(i)* ist also $\forall k \in \{0,1,\ldots,r\} : a_k 7^k \equiv a_k(-1)^k \pmod 4$. Damit bekommen wir

$$n \equiv \sum_{k=0}^{r} a_k 7^k \equiv \sum_{k=0}^{r} a_k(-1)^k \equiv Q_7^{alt} a_k \pmod 4.$$

□

(b) Aus (a) ist herzuleiten: *(i)* $3 \mid n \iff 3 \mid Q_7(n)$,
(ii) $4 \mid n \iff 4 \mid Q_7^{alt}(n)$.

Beweis. *(i)* $3 \mid n \iff n \equiv 0 \pmod 3 \overset{(a)}{\iff} Q_7(n) \equiv 0 \pmod 3 \iff 3 \mid Q_7(n)$.
(ii) $4 \mid n \iff n \equiv 0 \pmod 4 \overset{(a)}{\iff} Q_7^{alt}(n) \equiv 0 \pmod 4 \iff 4 \mid Q_7^{alt}(n)$. □

Übungsblatt 12

Aufgabe 43

Zu zeigen: Für jede Primzahl $p \in \mathbb{N}$ und alle ganzen Zahlen $a, b \in \mathbb{Z}$ ist $(a+b)^p \equiv a^p + b^p \pmod p$.

Beweis. Nach Satz (9.42) gilt für alle $x \in \mathbb{Z}$: $x^p \equiv x \pmod p$, falls p prim. Nun gilt

$$\begin{array}{rrl} & a^p & \equiv a \pmod p \\ + & b^p & \equiv b \pmod p \\ \hline & a^p + b^p & \equiv a+b \pmod p \end{array}$$

und außerdem ist nach Satz (9.42): $(a+b)^p \equiv a+b \pmod p$. Da $\equiv$ eine Äquivalenzrelation und insbes. transitiv ist, gilt $a^p + b^p \equiv (a+b)^p \pmod p$. □

Aufgabe 44

Gesucht sind die beiden letzten Ziffern der Dezimaldarstellung von $a := 123456789^{4921}$.
Besitzt a die Dezimaldarstellung $a = a_n a_{n-1} \ldots a_2 a_1 a_0)_{10}$, so ist $a \equiv (a_1 a_0)_{10} \pmod{100}$. Also brechnen wir $a \equiv 89 \pmod{100}$. Da 89 und 100 teilerfremd sind, gilt nach dem Satz von EULER (9.44): $89^{\varphi(100)} \equiv 1 \pmod{100}$. Wir müssen nun $\varphi(100)$, also die Anzahl der Zahlen aus $\{1,\ldots,100\}$ berechnen, die zu 100 teilerfremd sind.
Sei also $1 \le k \le 100$ und $\mathrm{ggT}(100,k) = 1$. Da $100 = 2^2 \cdot 5^2$ muß also gelten $2 \nmid k$ und $5 \nmid k$. Also muß k eine ungerade Zahl sein – davon gibt es 50 zwischen 1 und 100. Jede fünfte davon wird aber von 5 geteilt, so daß 40 Zahlen mit den gewünschten Eigenschaften übrigbleiben. Also $\varphi(100) = 40$.

Folglich gilt $89^{40} \equiv 1 \pmod{100}$. Wir können den Exponenten 4912 schreiben als $4921 = 123 \cdot 40 + 1$. Demnach ist

$$a^{4921} \equiv 89^{4921} \equiv \underbrace{(89^{40})^{123}}_{\equiv 1} \cdot 89 \equiv 1^{123} \cdot 89 \equiv 89 \pmod{100}.$$

Aufgabe 45

Seien $a = 2767198, b = 1716495$. Es ist der $\mathrm{ggT}(a,b)$ zu berechnen.

(a) Durch den Euklidischen Algorithmus:

$$\begin{aligned}
2767198 &= 1 \cdot 1716495 + 1050703\\
1716495 &= 1 \cdot 1050703 + 665792\\
1050703 &= 1 \cdot 665792 + 384911\\
665792 &= 1 \cdot 384911 + 104030\\
384911 &= 1 \cdot 280881 + 104030\\
280881 &= 2 \cdot 104030 + 72821\\
104030 &= 1 \cdot 72821 + 31209\\
72821 &= 2 \cdot 31209 + 10403\\
31209 &= 3 \cdot \boxed{10403} + 0
\end{aligned}$$

Damit ist $\mathrm{ggT}(a,b) = 10403$.

(b) Das Sieb des Eratosthenes:
Wir steichen aus der Liste der Zahlen von 2 bis 400 alle echten Vielfachen der Zahl 2, dann von $3, 5, 7, \ldots$ bis die nächste, noch nicht gestrichene Zahl größer als $\lfloor\sqrt{400}\rfloor = 20$ ist. Es bleiben alle 78 Primzahlen kleinergleich 400 übrig:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397

(c) ggT-Berechnung durch Primfaktorzerlegung:
Wir teilen a und b sukzessive durch alle Primzahlen kleiner als 400:

$$\begin{aligned}
a &= 2767198 & b &= 1716495\\
a_1 &= 2767198/2 = 1383599 & b_1 &= 1716495/3 = 572165\\
a_2 &= 1383599/7 = 197657 & b_2 &= 572165/5 = 114433\\
a_3 &= 197657/19 = 10403 & b_3 &= 114433/11 = 10403\\
a_4 &= 10403/101 = 103 & b_4 &= 10403/101 = 103\\
\Longrightarrow a &= 2 \cdot 7 \cdot 19 \cdot 101 \cdot 103 & \Longrightarrow a &= 3 \cdot 5 \cdot 11 \cdot 101 \cdot 103
\end{aligned}$$

Die Primfaktoren, die in a und b auftauchen sind $101, 103$. Damit ist $\mathrm{ggT}(a,b) = 101 \cdot 103 = 10403$.

Aufgabe 46

(a) $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} + \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ ist nicht definiert, da die Matrizen unterschiedliche Formate haben.

(b) $\begin{pmatrix} [1]_5 & [3]_5 & [7]_5 \\ [0]_5 & [2]_5 & [6]_5 \end{pmatrix} + \begin{pmatrix} [3]_5 & [2]_5 & [6]_5 \\ [12]_5 & [-3]_5 & [1]_5 \end{pmatrix} = \begin{pmatrix} [4]_5 & [0]_5 & [3]_5 \\ [2]_5 & [4]_5 & [2]_5 \end{pmatrix}$

(c) $\begin{pmatrix}1&2&3\\4&5&6\end{pmatrix}\cdot\begin{pmatrix}4&5\\6&8\\7&9\end{pmatrix}=\begin{pmatrix}37&48\\88&114\end{pmatrix}$

(d) $\begin{pmatrix}4&5\\6&8\\7&9\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\4&5&6\end{pmatrix}=\begin{pmatrix}24&33&42\\38&52&66\\43&59&75\end{pmatrix}$

(e) $\begin{pmatrix}1&2\\5&6\end{pmatrix}\cdot\begin{pmatrix}4&5\\6&8\\7&9\end{pmatrix}$ ist nicht definiert, da die Spaltenzahl (2) des ersten Faktors nicht mit der Zeilenzahl des zweiten Faktors (3) übereinstimmt.

(f) $\begin{pmatrix}[15]_7&[14]_7\\[35]_7&[-13]_7\end{pmatrix}\cdot\begin{pmatrix}[9]_7&[25]_7\\[5]_7&[93]_7\end{pmatrix}=\begin{pmatrix}[2]_7&[4]_7\\[5]_7&[2]_7\end{pmatrix}$

Übungsblatt 13

Aufgabe 47

Gegeben ist die Menge $M=\{1,2,3,4,5,6\}$.

(a) Gesucht ist die Adjazenzmatrix zu $\leq$ auf M. $A=(a_{ij})\in M_6(\mathbb{R})$ mit $a_{ij}=\begin{cases}1 & i\leq j,\\ 0 & \text{sonst.}\end{cases}$

$$A=\begin{pmatrix}1&1&1&1&1&1\\0&1&1&1&1&1\\0&0&1&1&1&1\\0&0&0&1&1&1\\0&0&0&0&1&1\\0&0&0&0&0&1\end{pmatrix}$$

(b) Gesucht ist die Relation auf M, die die folgende Adjazenzmatrix hat:

$$\begin{pmatrix}0&1&1&1&1&1\\1&0&1&1&1&1\\1&1&0&1&1&1\\1&1&1&0&1&1\\1&1&1&1&0&1\\1&1&1&1&1&0\end{pmatrix}$$

Es gilt hier offensichtlich $\forall x,y\in M:\ xRy\Longleftrightarrow a_{xy}=1\Longleftrightarrow x\neq y$, also ist $\neq$ die gesuchte Relation.

Aufgabe 48

Es sei R eine Relation auf der Menge $M=\{1,\ldots,n\}$, $n\in\mathbb{N}$, mit $A_R=(a_{ij})\in M_n(\mathbb{R})$ als Adjazenzmatrix.

(a) Zu zeigen: R reflexiv $\Longleftrightarrow\forall i\in M:\ a_{ii}=1$.

Beweis. R reflexiv $\Longleftrightarrow\forall i\in M:\ iRi\Longleftrightarrow\forall i\in M:\ a_{ii}=1$. □

(b) Zu zeigen: R symmetrisch $\Longleftrightarrow A_R$ ist symmetrisch.

Beweis. "$\Longrightarrow$" Sei also R symmetrisch. Dann gilt $\forall i,k\in M:\ iRk\Longrightarrow kRi$ und damit $\forall i,k\in M:\ a_{ik}=1\Longrightarrow a_{ki}=1$. Analog gilt $\forall i,k\in M:\ i\not Rk\Longrightarrow k\not Ri$ und damit $\forall i,k\in M:\ a_{ik}=0\Longrightarrow a_{ki}=0$.

"$\Leftarrow$" Sei A_R symmetrisch, also $\forall i,k \in M:\ a_{ki} = a_{ki}$. Dann gilt
$\forall i,k \in M:\ a_{ik} = 1 \Longrightarrow a_{ki} = 1 \Longleftrightarrow iRk \Longrightarrow kRi,$
also R symmetrisch. □

(c) Zu zeigen: R transitiv $\Longleftrightarrow \forall i,k,l \in M:\ a_{ik} \cdot a_{kl} \leq a_{il}$.

Beweis. "$\Longrightarrow$" Sei R transitiv und $i,k,l \in M$ beliebig. Sind $a_{ik} = a_{kl} = 0$, so ist $a_{ik} \cdot a_{kl} = 0$. Seien $a_{ik} = a_{kl} = 1$, dann gilt $iRk \wedge kRl$ und wegen der Transitivität von R auch iRl und damit $a_{il} = 1 \Longrightarrow a_{ik} \cdot a_{kl} = 1 \leq 1 = a_{il}$.
"$\Leftarrow$" Es gelte iRk und kRl für $i,k,l \in M$. Dann ist $a_{ik} = a_{kl} = 1$ und somit muß für $a_{il} = 1$ gelten. Also ist iRl und R ist transitiv. □

(d) Zu zeigen: Für die zu R inverse Relation R^{-1} gilt $A_{R^{-1}} = {}^tA_R$.

Beweis. Nach Definition der inversen Relation gilt $\forall i,k \in M:\ iR^{-1}k \Longleftrightarrow kRi$. Seien nun $A_{R^{-1}} = (b_{ik})$ und ${}^tA_R = (a_{ki})$ die darstellenden Matrizen. Für alle $i,k \in M$ gilt $b_{ik} = 1 \Longleftrightarrow iR^{-1}k \Longleftrightarrow kRi \Longleftrightarrow a_{ki} = 1$. Entsprechend gilt auch $b_{ik} = 0 \Longleftrightarrow a_{ki} = 0$. Also $\forall i,k \in M:\ b_{ik} = a_{ki}$ und damit $A_{R^{-1}} = {}^tA_R$. □

Aufgabe 49

Wir haben $A = \begin{pmatrix} 2 & -1 & 1 \\ -3 & 4 & -3 \\ -5 & 4 & -3 \end{pmatrix}$, $B = \begin{pmatrix} 1 & -1 & 1 \\ -3 & 3 & -3 \\ -5 & 5 & -5 \end{pmatrix} \in M_3(\mathbb{R})$.

(a) Wir berechnen $A \cdot B = B \cdot A = 0$ (die Nullmatrix), $A \cdot A = A$,

$$E_{12} \cdot A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot A = \begin{pmatrix} -3 & -4 & -3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{und}$$

$$E_{32} \cdot A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \cdot A = \begin{pmatrix} 0 & -1 & 0 \\ 0 & -3 & 0 \\ 0 & -4 & 0 \end{pmatrix}.$$

(b) Behauptung: A, B sind nicht invertierbar.

Beweis durch Widerspruch. Annahme: A ist invertierbar, also existiert ein A^{-1} mit $A \cdot A^{-1} = A^{-1} \cdot A = E_3$. Dann gilt aber auch
$A^{-1} \cdot \underbrace{(A \cdot B)}_{=0} = \underbrace{(A^{-1} \cdot A)}_{=E_3} \cdot B = B,$
also $B = 0$ — Widerspruch.
Durch analoge Argumentation erhält man, daß B nicht invertierbar ist. □

(c) Behauptung: $\forall n \in \mathbb{N}:\ A^n = A$.

Beweis durch Induktion. Induktionsanfang: $n = 1$ $A^1 = A$
Induktionsvoraussetzung: Für ein beliebiges $n \in \mathbb{N}$ gilt $A^n = A$.
Induktionsbehauptung: $A^{n+1} = A$.
Induktionsschritt: $A^{n+1} = A \cdot A^n \overset{\text{IV}}{=} A \cdot A = A$. □

Aufgabe 50

Sei $\mathcal{C} := \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \;\middle|\; a,b \in \mathbb{R} \right\} \subseteq M_2(\mathbb{R})$.

(a) Zu zeigen: Die Nullmatrix und die zweireihige Einheitsmatrix gehören zu $\mathcal{C}$, $\mathcal{C}$ ist abgeschlossen unter Matrizenaddition und -multiplikation.

Beweis. Wegen $0 = 0$ und $0 = -0$ sowie $1 = 1$ und $0 = -0$ gehören die Nullmatrix und die zweireihige Einheitsmatrix zu $\mathcal{C}$.
Seien $A := \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, $B := \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \in \mathcal{C}$. Dann ist $A+B = \begin{pmatrix} (a+c) & -(b+d) \\ (b+d) & (a+c) \end{pmatrix} \in \mathcal{C}$.
Außerdem ist $A \cdot B = \begin{pmatrix} (ac-bd) & -(ad+bc) \\ (ad+bc) & (ac-bd) \end{pmatrix} \in \mathcal{C}$. □

(b) Zu zeigen: $A = \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix} \in \mathcal{C}$ ist invertierbar und $A^{-1} \in \mathcal{C}$.

Beweis. Gesucht ist $B = \begin{pmatrix} u & x \\ v & y \end{pmatrix} \in \mathcal{C}$ mit $A \cdot B = E_2$. Also müssen wir die Gleichungssysteme $A\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ und $A\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ lösen. Dies liefert uns $B = \begin{pmatrix} \frac{1}{5} & \frac{2}{5} \\ -\frac{2}{5} & \frac{1}{5} \end{pmatrix} \in \mathcal{C}$. □

Wann ist eine allgemeine Matrix $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathcal{C}$ invertierbar?
Im Allgemeinen gilt: A invertierbar $\Longleftrightarrow \det A \neq 0 \Longleftrightarrow a^2 + b^2 \neq 0$, also wenn $a \neq 0$ oder $b \neq 0$ gilt. Es gilt dann $A^{-1} = \frac{1}{a^2+b^2} \cdot \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathcal{C}$. (Determinanten müssen wir noch nicht kennen!)

(c) Zu zeigen: Es gibt Matrix $I \in \mathcal{C}$ mit $I^2 + E_2 = 0$.

Beweis. Setze $I := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Dann ist $I \in \mathcal{C}$ und es gilt $I^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -E_2$ und damit $I^2 + E_2 = 0$. □

Übungsblatt 14

Aufgabe 51

Seien $A = \begin{pmatrix} 1 & 0 & 1 \\ -1 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix} \in M_3(\mathbb{R})$ und $b = \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} \in \mathbb{R}^3$.

(a) Zu zeigen: A ist invertierbar. Berechne außerdem A^{-1}.
Wir versuchen zunächst, A^{-1} zu berechnen:

	A			E_3			b
	1	0	1	1	0	0	2
$A_{21}(1)$	−1	2	1	0	1	0	1
	0	1	2	0	0	1	1
	1	0	1	1	0	0	2
V_{23}	0	2	2	1	1	0	3
	0	1	2	0	0	1	1
	1	0	1	1	0	0	2
$A_{23}(-2)$	0	1	2	0	0	1	1
	0	2	2	1	1	0	3
$A_{13}(\frac{1}{2})$	1	0	1	1	0	0	2
$A_{23}(1)$	0	1	2	0	0	1	1
	0	0	−2	1	1	−2	1

	A			E_3			b
	1	0	0	$\frac{3}{2}$	$\frac{1}{2}$	-1	$\frac{5}{2}$
	0	1	0	1	1	-1	2
$D_3(-\frac{1}{2})$	0	0	-2	1	1	-2	1
	1	0	0	$\frac{3}{2}$	$\frac{1}{2}$	-1	$\frac{5}{2}$
	0	1	0	1	1	-1	2
	0	0	1	$-\frac{1}{2}$	$-\frac{1}{2}$	1	$-\frac{1}{2}$
	$T(A)$			A^{-1}			0

Wegen $T(A) = E_3$ ist nach Satz (10.27) A invertierbar, A^{-1} wurde in der dritten Spalte berechnet.

(b) Gesucht sind alle Lösungen x des linearen Gleichungssystems $A \cdot x = b$.

Wir wissen $\text{Lös}(A,b) = \text{Lös}(T(A),c)$ mit $c = \begin{pmatrix} \frac{5}{2} \\ 2 \\ -\frac{1}{2} \end{pmatrix}$ wie es in Teil (a) berechnet wurde.

$T(A) \cdot x = c$ ist genau dann erfüllt wenn $x = c = \begin{pmatrix} \frac{5}{2} \\ 2 \\ -\frac{1}{2} \end{pmatrix}$, denn $T(A)$ ist ja gerade die Einheitsmatrix. Dies liefert uns $\text{Lös}(A,b) = \text{Lös}(T(A),c) = \{\begin{pmatrix} \frac{5}{2} \\ 2 \\ -\frac{1}{2} \end{pmatrix}\}$.

(c) Kann es ein $c \in \mathbb{R}^3$ geben, so daß $A \cdot x = c$ nicht lösbar ist?

Nein. Sei $c \in \mathbb{R}^3$ beliebig. Dann ist $A^{-1} \cdot c$ eine Lösung des LGSs, denn

$$A \cdot (A^{-1}c) = (A \cdot A^{-1})c = E_3 \cdot c = c.$$

(d) Stelle die Matrix A als ein Produkt von Elementarmatrizen dar.

Wie wir in (a) gesehen haben, gilt

$$\underbrace{D_3\left(-\frac{1}{2}\right) \cdot A_{23}(1) \cdot A_{13}\left(\frac{1}{2}\right) \cdot A_{32}(-2) \cdot V_{23} \cdot A_{21}(1)}_{=:G} \cdot A = G \cdot A = T(A) = E_3$$

und damit

$$\begin{aligned} A &= G^{-1} \cdot T(A) = G^{-1} \cdot E_3 = G^{-1} \\ &= \left(D_3\left(-\frac{1}{2}\right) \cdot A_{23}(1) \cdot A_{13}\left(\frac{1}{2}\right) \cdot A_{32}(-2) \cdot V_{23} \cdot A_{21}(1)\right)^{-1} \\ &= A_{21}(1)^{-1} \cdot V_{23}^{-1} \cdot A_{32}(-2)^{-1} \cdot A_{13}\left(\frac{1}{2}\right)^{-1} \cdot A_{23}(1)^{-1} \cdot D_3\left(-\frac{1}{2}\right)^{-1} \\ &= A_{21}(-1) \cdot V_{23} \cdot A_{32}(2) \cdot A_{13}\left(-\frac{1}{2}\right) \cdot A_{23}(-1) \cdot D_3(-2) \end{aligned}$$

Aufgabe 52

Seien $A := \begin{pmatrix} 1 & 0 & 1 & 1 & -1 \\ 2 & 1 & -1 & 1 & 0 \\ 3 & 1 & 0 & 2 & -1 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix} \in M_{4,5}(\mathbb{R})$ und $b = \begin{pmatrix} 2 \\ 0 \\ 2 \\ 0 \end{pmatrix}, b' = \begin{pmatrix} 1 \\ 0 \\ 2 \\ 0 \end{pmatrix} \in \mathbb{R}^4$.

Gesucht sind die Lösungsmengen von $A \cdot x = b$ und $A \cdot x = b'$.

Wir benutzen den Gauss-Algorithmus:

A					b	b'
1	0	1	1	-1	2	1
2	1	-1	1	0	0	0
3	1	0	2	-1	2	2
1	1	0	0	0	0	0
$\downarrow$ Elementare Zeilenumformungen $\downarrow$						
1	0	0	1	$-\frac{1}{2}$	1	0
0	1	0	-1	$\frac{1}{2}$	-1	0
0	0	1	0	$-\frac{1}{2}$	1	0
0	0	0	0	0	0	1
$T(A)$					c	c'

Nun lösen wir das LGS $T(A)\cdot x = c$:

$$\begin{array}{rrrrrrr} x_1 & & & +x_4 & -\frac{1}{2}x_5 & = & 1 \\ & x_2 & & -x_4 & +\frac{1}{2}x_5 & = & -1 \\ & & x_3 & & -\frac{1}{2}x_5 & = & 1 \\ \hline \multicolumn{7}{l}{\text{setze } x_4 = r \in \mathbb{R} \text{ und } x_5 = 5 \in \mathbb{R} \text{ beliebig.}} \end{array}$$

und wir erhalten:

$$\begin{aligned} x_3 &= 1+\frac{1}{2}s \\ x_2 &= -1+r-\frac{1}{2}s \\ x_1 &= 1-r+\frac{1}{2}s \end{aligned}$$

und damit

$$\text{Lös}(A,b) = \left\{ \left(\begin{array}{c} 1-r+\frac{1}{2}s \\ -1+r-\frac{1}{2}s \\ 1+\frac{1}{2}s \\ r \\ s \end{array} \right) \middle| \, r,s \in \mathbb{R} \right\}.$$

Das LGS $T(A)\cdot x = c'$ ist nicht lösbar, da sonst $0=1$ folgen würde. Also ist $\text{Lös}(A,b') = \emptyset$.

Aufgabe 53

Zu lösen ist das LGS $\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 1 & 1 & 0 \end{pmatrix} \cdot x = \begin{pmatrix} 3 \\ 4 \\ 2 \end{pmatrix}$ über $\mathbb{Z}_5$. Hierbei stehen die Zahlen für die entsprechenden Restklassen modulo 5.
Modulo 5 gelten insbesondere $2\cdot 3 = 4\cdot 4 = 1$, also $2^{-1}=3,\ 3^{-1}=2,\ 4^{-1}=4$. Nun führen wir den Gauss-Algorithmus wie gewohnt durch:

A			b
1	0	2	3
0	1	3	4
1	1	0	2
1	0	2	3
0	1	3	4
0	1	3	4
1	0	2	3
0	1	3	4
0	0	0	0

Wir setzen $x_3 = r \in \mathbb{Z}_5$ beliebig und erhalten

$$\begin{aligned} x_3 &= r \\ x_2 &= 4+2r \\ x_1 &= 3+3r \end{aligned}$$

und damit

$$\begin{aligned} \text{Lös}(A,b) &= \left\{ \begin{pmatrix} 3+3r \\ 4+2r \\ r \end{pmatrix} \middle| \, r \in \mathbb{Z}_5 \right\} \\ &= \{ \begin{pmatrix} 3 \\ 4 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 4 \end{pmatrix} \} \end{aligned}$$

Es gibt also genau 5 Lösungen.

Aufgabe 54

Moderne Kommunikationsgeräte (wie z.B. Handies, Satelliten, CD-Player) arbeiten digital, d.h., alle Daten werden als Folge von 0 und 1 (sog. Bitströmen) dargestellt. Ein Problem ist dabei das Erkennen von Übertragungsfehlern, d.h. statt des gesendeten Bits a kommt das Bit $1-a$ an. Solche Probleme werden in der Codierungstheorie behandelt. Dazu nutzt man lineare Gleichungssysteme und Matrizen.

1. Die einfachste Art, einen Fehler zu erkennen, ist, ein Bit a dreimal zu schicken, also *aaa* statt a. Drei Bits $x_1x_2x_3$ werden dann vom Empfänger als Einheit gelesen. Das Wort ist richtig empfangen worden, wenn gilt

   (4) $\qquad x_2 = x_3$ und $x_1 = x_3$.

   Schreiben Sie diese Gleichungen in eine Matrixschreibweise vom Typ

   $$H \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

   um, wobei alle Einträge *modulo* 2 gerechnet werden, da sie Bits darstellen! Bestimmen Sie die Menge aller Lösungen des Gleichungssystems (4) *in* $\mathbb{Z}_2$. Die Elemente dieser Lösungsmenge sind 3-Bit-Worte $x_1x_2x_3$ und werden *Worte des Codes* genannt.

   Lösung: *Durch Umformen erhält man*
   $\begin{matrix} 0\cdot x_0+1\cdot x_2+(-1)\cdot x_3=0 \\ 1\cdot x_0+0\cdot x_2+(-1)\cdot x_3=0 \end{matrix}$ *, und damit* $H = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$.
   Dabei zu beachten: $-1 \equiv 1 \bmod 2$. *Diese Matrix ist bereits in Treppenform, wenn man die beiden Zeilen tauscht. Als Lösungen ergeben sich* ${}^t(0,0,0)$ *(bei Wahl* $x_3 = 0$*) und* ${}^t(1,1,1)$ *(bei Wahl* $x_3 = 1$*). Der Code umfasst also die Worte* ${}^t(0,0,0)$ *und* ${}^t(1,1,1)$.

2. Kommt nun ein Wort an, dass kein Wort des Codes ist, so wird es korrigiert. Das geschieht wie folgt: zwei Bits sind gleich, ein Bit ist davon verschieden. Das *ursprüngliche Bit* ist dann gleich dem Wert, der zweimal vorkommt. Bsp: empfangen 101, dann ist das ursprünglich gesendete Bit 1. Wie lautet also der ursprünglich gesendete Bitstrom, wenn man folgende 3-Bit-Folge empfängt?

   101 111 001 010 110 001 100

Lösung: *Fehler sind aufgetreten in allen* 3*-Tupeln außer dem zweiten:*

empfangen:	101	111	001	010	110	001	100
korrigiert :	1**1**1	111	00**0**	0**0**0	11**1**	00**0**	**0**00
Bitstrom :	1	1	0	0	1	0	0.

3. Das Problem ist: statt ursprünglich ein Bit werden nun 3 Bit gesendet, d.h., die Nachricht wird um den Faktor 3 aufgebläht. Mit sogenannten *Hamming-Codes* kann man einen kleineren Faktor erreichen. Man sendet immer 4 Bits x_1,x_2,x_3,x_4 und fügt drei Kontrollbits y_1,y_2,y_3 hinzu. Ein Codewort ist dann ein 7-Bit-Wort $x_1x_2x_3x_4y_1y_2y_3$, das folgendes Gleichungssystem erfüllt:

$$(5) \qquad \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

In der *i*-ten Spalte der Matrix steht also gerade die Zahl *i* in binärer Schreibweise (${}^t(0,0,1)$ steht also für binär (001), d.h. 1)! Codieren Sie alle 4-Bit-Worte $x_1x_2x_3x_4$ mit diesem Code, indem Sie y_1,y_2,y_3 bestimmen, so dass ${}^t(x_1,x_2,x_3,x_4,y_1,y_2,y_3)$ eine Lösung von (5) ist.

Lösung: *Durch die Matrixschreibweise ist folgendes Gleichungssystem gegeben*

$$\begin{aligned} 0\cdot x_1+0\cdot x_2+0\cdot x_3+1\cdot x_4+1\cdot y_1+1\cdot y_2+1\cdot y_3 &= 0 \\ 0\cdot x_1+1\cdot x_2+1\cdot x_3+0\cdot x_4+0\cdot y_1+1\cdot y_2+1\cdot y_3 &= 0, \\ 1\cdot x_1+0\cdot x_2+1\cdot x_3+0\cdot x_4+1\cdot y_1+0\cdot y_2+1\cdot y_3 &= 0 \end{aligned}$$

dass man nach y_1,y_2,y_3 *umformt:*

$$\begin{aligned} y_1 &= & x_2 & +x_3 & +x_4 \\ y_2 &= x_1 & & +x_3 & +x_4 \\ y_3 &= x_1 & +x_2 & & +x_4 \end{aligned}.$$

Dann ergeben sich folgende Codeworte:

x_1	x_2	x_3	x_4	y_1	y_2	y_3	x_1	x_2	x_3	x_4	y_1	y_2	y_3
0	0	0	0	0	0	0	1	0	0	0	0	1	1
0	1	0	0	1	0	1	1	1	0	0	1	1	0
0	0	1	0	1	1	0	1	0	1	0	1	0	1
0	1	1	0	0	1	1	1	1	1	0	0	0	0
0	0	0	1	1	1	1	1	0	0	1	1	0	0
0	1	0	1	0	1	0	1	1	0	1	0	0	1
0	0	1	1	0	0	1	1	0	1	1	0	1	0
0	1	1	1	1	0	0	1	1	1	1	1	1	1

4. Zeigen Sie: Addiert man zwei Codeworte $a,b \in \mathbb{Z}_2^7$, so ist das Wort $c = a+b$ auch ein Codewort, d.h. eine Lösung von (5).

Lösung: *Seien* $a,b \in \mathbb{Z}_2^7$ *zwei Lösungsvektoren des Gleichungssystems. Wir schreiben für die Matrix einfach* $H \in M_{3,7}(\mathbb{Z}_2)$*. Dann gilt:* $H \cdot a = 0$ *und* $H \cdot b = 0$*, also*

$$H \cdot (a+b) = H \cdot a + H \cdot b = 0+0 = 0,$$

d.h. auch $a+b$ *ist wieder eine Lösung.(Vgl. Satz (10.37)).*

5. Man kann die fehlerhafte Übertragung des i-ten Bits ($1 \leq i \leq 7$) beim Codewort $a = {}^t(x_1, x_2, x_3, x_4, y_1, y_2, y_3)$ wie folgt in Formeln darstellen: man addiert den Einheitsvektor $e_i \in \mathbb{Z}_2^7$ (in Zeile i steht eine 1, sonst 0) zu a. Zeigen Sie: Multipliziert man die Matrix aus (5) von rechts mit $a + e_i$, so ist die Lösung gerade der Vektor, der transponiert die Binärdarstellung von i ist.

   Lösung: *Sei* $e_i = {}^t(0, \ldots, 0, 1, 0, \ldots, 0)$ *der Einheitsvektor, der in der i-ten Zeile* ($1 \leq i \leq 7$) *eine* 1 *enthält. Dann gilt für einen Lösungsvektor* $a \in \mathbb{Z}_2^7$ *gerade:*

   $$H \cdot (a + e_i) = H \cdot a + H \cdot e_i = 0 + H \cdot e_i = H_i,$$

   wobei H_i *die i-te Spalte von H bezeichnet. Die Matrix H ist aber so konstruiert, dass in der i-ten Spalte gerade die Zahl i binär codiert steht.*

6. Man erhält also die ursprünglichen Bits zurück, indem man jeden 7-stelligen empfangenen Bit-Vektor von rechts an die Matrix aus (5) multipliziert. Ist das Ergebnis ${}^t(0,0,0)$, so ist das empfangene Wort korrekt, und man nimmt die ersten vier Bit als ursprüngliche Nachricht. Andernfalls erhält man als Ergebnis den Index des falsch übertragenen Bits. Dieses Bit korrigiert man: aus 0 mache 1 bzw. aus 1 wird 0. Dann nimmt man die ersten vier Bit als ursprüngliche Nachricht. Wie lautet also die ursprünglich gesendete Folge von 4 Bits, wenn man folgende 7-Bit-Folge empfängt?

   ${}^t(0,1,1,0,0,1,1)$ ${}^t(0,1,1,0,1,0,1)$

   Lösung: *Die Decodierung des ersten Vektors ergibt:*

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

   d.h. der Vektor wurde fehlerfrei übertragen, die ursprünglichen vier Bits lauten: 0110. *Für den zweiten Vektor haben wir aber:*

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

   d.h. das dritte Bit ist fehlerhaft. Korrigiert lautet der Vektor $(0,1,\mathbf{0},0,1,0,1)$*, also wurde ursprünglich* 0100 *gesendet.*

7. Um welchen Faktor wird die ursprüngliche Nachricht bei diesem Hamming-Code aufgebläht?

   Lösung: *Statt* 4 *Bit werden* 7 *Bit gesendet, also wird die Nachricht um den Faktor* $\frac{7}{4} = 1.75 < 2$ *aufgebläht.*