

**Lösungen der Übungsaufgaben in
Diskrete Mathematik kompakt
(Bernd Baumgarten, De Gruyter, 2024)
– Kapitel 5: Zahlen und Anzahlen –**

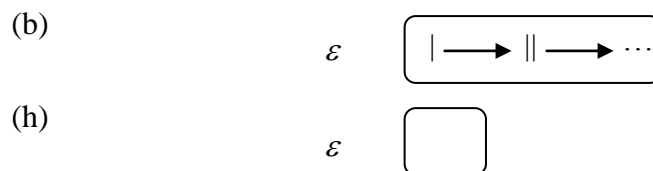
Bitte beachten Sie:

- Versuchen Sie stets, die Aufgabe zunächst selbst zu lösen! Das Anschauen einer gelösten Übungsaufgabe *ohne vorherigen eigenen ernsthaften Bearbeitungsversuch* nützt Ihnen hinsichtlich des Lernerfolgs oft nicht mehr als der Genuss einer Tasse Kaffee: Es erzeugt einfach nur vorübergehend ein angenehmes Gefühl, hinterlässt aber keinen bleibenden Effekt.
- Zu jeder Aufgabe kann es verschiedene korrekte Lösungen bzw. Lösungswege und für jede Lösung mehrere Schreibweisen geben. Daher sind die in der Folge vorgestellten Lösungen durchweg nur als Beispiele zu verstehen.
- Zusätzliche Erklärungen stehen in eckigen Klammern [...].
- Auch in Übungsaufgaben können Fehler stecken. Bitte beachten Sie die eventuelle Korrigenda-Datei des Verlages.

5.1 Peano-Axiome

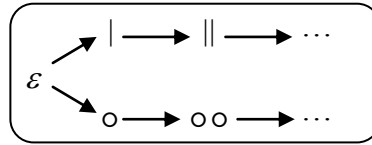
Wir geben hier zu jedem ausgelassenen Axiom jeweils ein oder zwei der vorgeschlagenen Modelle an, die von den natürlichen Zahlen verschieden sind aber die verbleibenden Axiome erfüllen (das ausgelassene Axiom jedoch nicht). Solch ein Modell gibt die Grundmenge (das Universum) an, darauf eine Nachfolger-Relation und eine ausgewählte Menge der Objekte mit der Eigenschaft „natürliche Zahl“. Dazu kommt jeweils eine kleine Illustration des Modells in welcher die Zahlenmenge eingerahmt ist:

Ax. (1) auslassen: Interpretationen (b) und (h)



Ax. (2) auslassen: Interpretationen (c) und (g)

(c)



(g)



Dabei sind die Axiome wie folgt modifiziert:

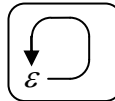
$$(3') \quad \forall m, n \in \mathbb{N}_0 \quad (succ(m, n) \rightarrow n \neq 0)$$

$$(4') \quad \forall m, n \in \mathbb{N}_0 \quad [\exists k \in \mathbb{N}_0 \quad (succ(m, k) \wedge succ(n, k))] \rightarrow m = n$$

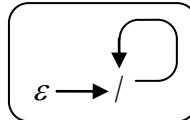
$$(5') \quad \forall M \quad ((M \subseteq \mathbb{N}_0 \wedge 0 \in M \wedge (\forall m \in M, n \in \mathbb{N}_0 \quad (succ(m, n) \rightarrow n \in M))) \Rightarrow M = \mathbb{N}_0)$$

Antwort auf die Zusatzfrage: In (c) ist *succ* immer noch linkstotal. In (g) ist *succ* immer noch rechtseindeutig. Diese beiden Eigenschaften von *succ* könnten also getrennt voneinander in den Peano-Axiomen postuliert werden, und die Axiome wären dann immer noch unabhängig.

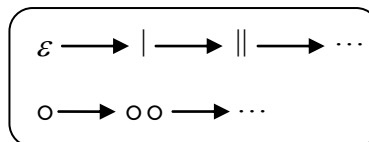
Ax. (3) auslassen: Interpretation (f)



Ax. (4) auslassen: Interpretation (e)



Ax. (5) auslassen: Interpretation (d)



5.2 Addition und Nachfolger

Die Aussage gilt für $n = 0$:

$$0 + 1 = plus_0(1) = plus_0(succ(0)) = succ(plus_0(0)) = succ(0)$$

Es gelte $succ(n) = n + 1$.

Dann gilt auch $succ(succ(n)) = succ(n) + 1$, denn

$$\begin{aligned} succ(n) + 1 &= plus_{succ(n)}(1) \\ &= plus_{succ(n)}(succ(0)) \\ &= succ(plus_{succ(n)}(0)) \\ &= succ(succ(n)) . \end{aligned}$$

5.3 Ordnungsrelationen auf natürlichen Zahlen

Nach Satz 5.2 gilt $m \leq n \Leftrightarrow \exists d \in \mathbb{N}_0 : m + d = n$.

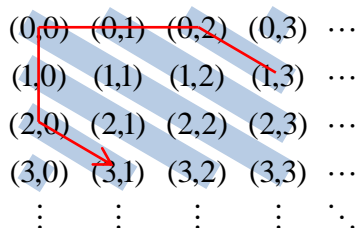
Für ein $d \in \mathbb{N}_0$ mit $m + d = n$ ist entweder $d = 0$, also $m + d = n \Leftrightarrow m = m + 0 = n$, oder $d \in \mathbb{N}$, also nach Satz 5.2 $m + d = n \Leftrightarrow m < n$.

Also gilt auch $\exists d \in \mathbb{N}_0 : m + d = n \Leftrightarrow m = n \vee m < n$.

5.4 Ordnungsrelationen und Vorgänger auf ganzen Zahlen

- a) (i) a. $[(0,0)]_{\sim} < [(1,0)]_{\sim}$
 b. $[(0,1)]_{\sim} < [(0,0)]_{\sim}$
 (ii) a. $[(i,k)]_{\sim} < [(m,n)]_{\sim} \Rightarrow [(succ(i),k)]_{\sim} < [(succ(m),n)]_{\sim}$
 b. $[(i,k)]_{\sim} < [(m,n)]_{\sim} \Rightarrow [(i,succ(k))]_{\sim} < [(m,succ(n))]_{\sim}$
 c. $[(i,k)]_{\sim} < [(m,n)]_{\sim} \Rightarrow [(succ(i),succ(k))]_{\sim} < [(m,n)]_{\sim}$
 d. $[(i,k)]_{\sim} < [(m,n)]_{\sim} \Rightarrow [(i,k)]_{\sim} < [(succ(m),succ(n))]_{\sim}$
 e. $([(i,k)]_{\sim} < [(m,n)]_{\sim} \wedge [(m,n)]_{\sim} < [(r,s)]_{\sim}) \Rightarrow [(i,k)]_{\sim} < [(r,s)]_{\sim}$

[Gesucht wird im Prinzip eine induktive Definition der Quadrupel (i,k,m,n) mit Komponenten in \mathbb{N}_0 , für die $[(i,k)]_{\sim} < [(m,n)]_{\sim}$, d.h. $i + n < k + m$ bzw. $i - k < m - n$ gilt (vgl. (b) unten). Bildlich gesehen sollen in der „unendlichen Matrix“



die Einträge in eine solche Relation $<$ gebracht werden, dass $(i,k) < (m,n)$ genau dann gilt, wenn die (blau angedeutete) Haupt- oder Nebendiagonale von (i,k) rechts oberhalb der von (m,n) liegt.

Wie „kommt man“ z.B. von $(1,3)$ nach links unten zu dem größeren Paar $(3,1)$?

In der obigen Lösung sorgen (i.b) und (ii.b) für $(0,0) < (0,1)$ und $(0,1) < (0,2)$. Die Transitivität in (ii.e) liefert $(0,0) < (0,2)$. Analog erhalten wir $(0,0) < (2,0)$ durch (i.a), (ii.a) und (ii.e). Die Transitivität in (ii.e) sorgt nun für $(0,2) < (2,0)$.

Von den bisher verglichenen Zahlenpaaren $(0,2)$ und $(2,0)$ aus können wir uns nun „auf den jeweiligen Diagonalen bewegen“, ohne dass die Ungleichung verloren geht: (ii.c) liefert den Übergang von $(0,2) < (2,0)$ zu $(1,3) < (2,0)$ und (ii.d) den weiteren Übergang zu $(1,3) < (3,1)$.]

$-2 < -1$: Wegen (i.b) $-1 = [(0,1)]_{\sim} < [(0,0)]_{\sim} = 0$ gilt mit (ii.b)
 $-2 = [(0,2)]_{\sim} = [(0,succ(1))]_{\sim} < [0,succ(0)]_{\sim} = [(0,1)]_{\sim} = -1$.

$-1 < 1$: Wegen (i.b) $-1 = [(0,1)]_{\sim} < [(0,0)]_{\sim} = 0$ und (i.a) $0 = [(0,0)]_{\sim} < [(1,0)]_{\sim} = 1$ gilt mit (ii.e) $-1 = [(0,1)]_{\sim} < [(1,0)]_{\sim} = 1$.

- b) $[(i,k)]_{\sim} < [(m,n)]_{\sim} :\Leftrightarrow i + n < k + m$ (letzteres in den natürlichen Zahlen interpretiert!),

[da $[(i,k)]_{\sim}$ dem gewohnten $i - k$ entsprechen soll, und wegen der gewohnten Ungleichungsrechnung $i - k < m - n \Leftrightarrow i + n < k + m$.

Dabei ist aber streng genommen noch zu beweisen, dass dies wirklich eine Definition (wohldefiniert) ist, also unabhängig von der Wahl des Repräsentanten der Äquivalenzklasse, d.h.

$$[(i,k)]_{\approx} < [(m,n)]_{\approx} \wedge (i,k) \approx (i',k') \wedge (m,n) \approx (m',n) \Rightarrow [(i',k')]_{\approx} < [(m',n')]_{\approx}.$$

Anders ausgedrückt: \approx muss eine Kongruenzrelation bezüglich $<$ sein.]

$-2 < -1$: In \mathbb{N}_0 gilt $m < \text{succ}(m)$, also $1 < 2$ bzw. $0+1 < 2+0$ bzw. $[(0,2)]_{\approx} < [(0,1)]_{\approx}$, d.h. in Kurzform $-2 < -1$.

$-1 < 1$: In \mathbb{N}_0 gilt $m < \text{succ}(m)$ und nach einem Induktionsschritt auch $m < \text{succ}(\text{succ}(m))$. Somit gilt $0 < 2$ bzw. $0+0 < 1+1$ bzw. $[(0,1)]_{\approx} < [(1,0)]_{\approx}$, d.h. in Kurzform $-1 < 1$.

c) $\text{pred}([(i,k)]_{\approx}) := [(i, \text{succ}(k))]_{\approx}$

Dabei bleibt aber noch zu beweisen, dass diese „Definition“ von der Wahl des Repräsentanten der Äquivalenzklasse unabhängig ist.

Für eine natürliche Zahl $n > 0$ ist $\text{pred}(n) = [(n,1)]_{\approx} = \text{pred}[(n,0)]_{\approx}$, wobei das linke pred das der natürlichen Zahlen und das rechte das der neu konstruierten ganzen Zahlen sein soll.

5.5 Zahlen-Paradoxien mit Kombinatorik und Wohlordnung

- a) Sei M die Menge der uninteressanten natürlichen Zahlen. Dann hat M ein kleinstes Element n , die kleinste aller uninteressanten Zahlen. Dies ist offenbar eine nicht triviale Eigenschaft, die n interessant macht – ein Widerspruch.
- b) Die kleinste natürliche Zahl, die sich nicht mit einer Folge von bis zu einhundert-fünfundzwanzig Zeichen beschreiben lässt, hat weniger als 125 Zeichen und beschreibt die Zahl scheinbar eindeutig, im Widerspruch dazu, dass es eine der Zahlen ist, für die 125 Zeichen nicht ausreichen. Dieses Paradoxon ist in ähnlicher Form als **Berrys Paradoxon** bekannt.

5.6 Negativenbildung in den ganzen Zahlen

- a) Wir haben zu zeigen, dass für je zwei natürliche Zahlen i, k ein passendes $n \in \mathbb{N}_0$ existiert, so dass $(i,k) \approx (n,0)$ oder $(i,k) \approx (0,n)$, also $i+n=k$ oder $i=k+n$.
Nach dem Wohlordnungssatz 5.4 (oder auch bereits Lemma 5.3) hat $\{i,k\}$ ein kleinstes Element. Ist dieses Element i , so gilt $i \leq k$. Nach Satz 5.2 existiert dann ein $n \in \mathbb{N}_0$ derart, dass $i+n=k$. Ist dagegen k das kleinste Element von $\{i,k\}$, so folgt analog $i=k+n$.
- b) Ist $k \leq i$ und (s.o.) $k+n=i$, so ist $-[(i,k)]_{\approx} = -[(n,0)]_{\approx} = [(0,n)]_{\approx} = [(k,i)]_{\approx}$, und analog im Fall $i \leq k$.
[Alternativ kann man argumentieren, dass $[(i,k)]_{\approx} + [(k,i)]_{\approx} = [(i+k, k+i)]_{\approx} = 0$.]
- c) Ist $m = [(i,k)]_{\approx}$ und $n = [(r,s)]_{\approx}$, so gilt

$(-m) \cdot n = (-[(i,k)]_{\approx}) \cdot [(r,s)]_{\approx}$	per Einsetzung
$= [(k,i)]_{\approx} \cdot [(r,s)]_{\approx}$	unter Verwendung von Aufgabenteil (b)
$= [(k \cdot r + i \cdot s, k \cdot s + i \cdot r)]_{\approx}$	gemäß der Definition der Multiplikation in \mathbb{Z}
$= [(i \cdot s + k \cdot r, i \cdot r + k \cdot s)]_{\approx}$	wegen der Kommutativität der Addition in \mathbb{N}_0
$= -[(i \cdot r + k \cdot s, i \cdot s + k \cdot r)]_{\approx}$	unter Verwendung von Aufgabenteil (b)
$= -([(i,k)]_{\approx} \cdot [(r,s)]_{\approx})$	gemäß der Definition der Multiplikation in \mathbb{Z}
$= -(m \cdot n)$	per Einsetzung

5.7 Rationale Zahlen und Dezimalbrüche

Für eine Dezimalzahl $z = a_k a_{k-1} \dots a_0, b_1 b_2 \dots b_l \overline{c_1 c_2 \dots c_m}$, mit periodischer Dezimalbruchentwicklung rechnet man $(10^m - 1) \cdot z = d_{k+m} d_{k+m-1} \dots d_0, e_1 e_2 \dots e_l$ aus mit Dezimalziffern $d_i, i = 0, \dots, k+m$ und $e_i, i = 1, \dots, l$. Hierbei ist jeweils die Dezimaldarstellung gemeint.

Für die natürlichen Zahl $n = d_{k+m} d_{k+m-1} \dots d_0 e_1 e_2 \dots e_l$ (Dezimaldarstellung) gilt dann

$$n = 10^l \cdot (10^m - 1) \cdot z, \text{ also } z = \frac{n}{10^l \cdot (10^m - 1)} \in \mathbb{Q}.$$

Der „naive“ Algorithmus der schriftlichen Division einer ganzen Zahl durch eine natürliche Zahl n (d.h. ohne Beachtung einer Periode) läuft so lange, bis kein Rest mehr bleibt, was eventuell nie passiert. Im letzteren Fall läuft er endlos.

- Endet er, ist das Ergebnis eine Zahl mit abbrechender Dezimalbruchentwicklung $a_1 a_2 \dots a_k, a_{k+1} a_{k+2} \dots a_{k+l} 0 \dots 0$ (mit m Nullen am Ende, wobei $m \geq 0$), wegen

$$a_1 a_2 \dots a_k, a_{k+1} a_{k+2} \dots a_{k+l} 0 \dots 0 = 10^{-(l+m)} \cdot a_1 a_2 \dots a_k, a_{k+1} a_{k+2} \dots (a_{k+l} - 1), \overline{9}$$

(problemlos: ggf. $l = 0$) also auch eine (eindeutige) periodische Zahl.

- Endet der Divisionsalgorithmus hingegen nicht, so müssen sich irgendwann die (nur endlich vielen möglichen unterschiedlichen) Reste $1, 2, \dots$ oder $n-1$ irgendwann wiederholen, weshalb sich die entsprechenden Dezimalziffern des Ergebnisses zwischen diesen Wiederholungen ab dann auch periodisch wiederholen müssen.

5.8 Ordnungsrelationen auf rationalen Zahlen

Wir definieren

$$[(i,k)]_{\equiv} < [(m,n)]_{\equiv} :\Leftrightarrow \begin{cases} i \cdot n < k \cdot m & \text{wenn } k \cdot n > 0 \\ k \cdot m < i \cdot n & \text{wenn } k \cdot n < 0 \end{cases} \text{ und}$$

$$[(i,k)]_{\equiv} \leq [(m,n)]_{\equiv} :\Leftrightarrow \begin{cases} i \cdot n \leq k \cdot m & \text{wenn } k \cdot n > 0 \\ k \cdot m \leq i \cdot n & \text{wenn } k \cdot n < 0 \end{cases},$$

wobei jeweils die linke Ungleichung in den neuen rationalen Zahlen und die rechten in den ganzen Zahlen zu interpretieren sind. Dies natürlich deswegen, weil $[(i,k)]_{\equiv}$ dem schulmäßigen Bruch i/k entspricht.

[Die entgegengesetzten Ungleichungen in den Alternativen sind dadurch bedingt, dass beispielsweise $(-2) \cdot 3 < 1 \cdot 4$ bei beidseitiger Division durch die negative Zahl $(-2) \cdot 4$ in die entgegen gerichtete Ungleichung $3/4 > 1/(-2)$, also $1/(-2) < 3/4$ übergeht.

Wieder kann man beweisen, dass dies wirklich Definitionen (wohldefinierte Beschreibungen) sind, vgl. Aufgabe 5.4.]

5.9 Irrationale Zahlen

Annahme: $\sqrt{6} = q/r$ mit $q, r \in \mathbb{Z}$.

Wir kürzen den Bruch so, dass $\sqrt{6} = a/b$, wobei a und b keine Teiler gemeinsam haben. Dann gilt $6 = a^2/b^2$, $a^2 = 6 \cdot b^2$, 2 teilt a^2 und daher auch a , so dass mit einer natürlichen Zahl c gilt: $a = 2 \cdot c$. Also gilt $4 \cdot c^2 = 6 \cdot b^2$, $2 \cdot c^2 = 3 \cdot b^2$. Somit sind b^2 und auch b gerade Zahlen. Insgesamt haben a und b den Teiler 2 gemeinsam, im Widerspruch zu ihrer Wahl. Somit muss die Annahme falsch und $\sqrt{6}$ irrational sein.

Annahme: $\sqrt{3} - \sqrt{2} = q/r$ mit $q \in \mathbb{Z}$, $r \in \mathbb{N}$.

Wir kürzen den Bruch, so dass $\sqrt{3} - \sqrt{2} = a/b$, wobei a und b keine Teiler gemeinsam haben.

Dann gilt

$$\sqrt{3} = \frac{a + \sqrt{2} \cdot b}{b}, \quad 3 = \frac{a^2 + 2 \cdot \sqrt{2} \cdot b + b^2}{b^2}, \quad \text{und damit} \quad \frac{2 \cdot b^2 - a^2}{2 \cdot b} = \sqrt{2}, \quad \text{also } \sqrt{2} \text{ rational, im}$$

Widerspruch zu Satz 5.6. Somit muss die Annahme falsch und $\sqrt{3} - \sqrt{2}$ irrational sein.

5.10 Division in Dedekind'schen Schnitten

Wir definieren für einen Schnitt $S \neq 0^*$ das multiplikative Inverse S^{-1} mit $S \cdot S^{-1} = 1^*$ und setzen dann $S_1 / S_2 := S_1 \cdot S_2^{-1}$, und zwar wie folgt:

Für $S < 0^*$ sei $\hat{S} := \{1/x \mid x < 0 \wedge x \notin S\}$, für $S > 0^*$ sei $\hat{S} := \{1/x \mid x \notin S\} \cup \{x \mid x \leq 0\}$, und in beiden Fällen sei dann $S^{-1} := \hat{S} \setminus \{\sup \hat{S}\}$.

[Wir prüfen am Beispiel $S = (-\infty, -1/2)$ nach:

$$\hat{S} = \{1/x \mid -1/2 \leq x < 0\} = (-\infty, -2] \quad \text{und} \quad S^{-1} = (-\infty, -2)$$

und am Beispiel $T = (-\infty, 3)$:

$$\hat{T} = \{1/x \mid 3 \leq x\} \cup (-\infty, 0] = (0, 1/3] \cup (-\infty, 0] = (-\infty, 1/3] \quad \text{und} \quad T^{-1} = (-\infty, 1/3]]$$

Dann ist z.B. für $S > 0^*$ (und, wie man leicht sieht, damit auch $S^{-1} > 0^*$)

$$\begin{aligned} S \cdot S^{-1} &= \{x \cdot y \mid x \in S \wedge x \geq 0 \wedge y \in S^{-1}\} \\ &= \{x/y \mid x \in S \wedge x \geq 0 \wedge y \notin S \wedge y \geq 0\} \cup (-\infty, 0] \end{aligned}$$

[Die x kommen von unten und die y von oben beliebig dicht aneinander heran, so dass x/y beliebig dicht von unten an 1 herankommt, so dass $S \cdot S^{-1} = \{z \in \mathbb{Q} \mid z < 1\} = 1^*$.]

5.11 Rechnen im Komplexen

- a)
- i. $= (3+1) + (-2 \cdot +4) \cdot i = 4 + 2 \cdot i$
 - ii. $= (3-1) + (-2-4) \cdot i = 2 - 6 \cdot i$
 - iii. $= (3 \cdot 1 - ((-2) \cdot 4) + (3 \cdot 4 - 2 \cdot 1) \cdot i$
 $= 11 + 10 \cdot i$
 - iv. $= \frac{3-2 \cdot i}{1+4 \cdot i} \cdot \frac{1-4 \cdot i}{1-4 \cdot i} = \frac{(3-2 \cdot i) \cdot (1-4 \cdot i)}{1^2 - (4 \cdot i)^2}$
 $= \frac{(3 \cdot 1 - (-2) \cdot (-4)) + (3 \cdot (-4) + (-2) \cdot 1) \cdot i}{1+16}$
 $= -\frac{5}{17} - \frac{14}{17} \cdot i$
- b)
- i. $(x + y \cdot i)^3 = x^3 + 3x^2y \cdot i + 3xy^2 \cdot i^2 + y^3 \cdot i^3$
 $= x^3 - 3xy^2 + (3x^2y - y^3) \cdot i$
 $(r \cdot (\cos \varphi + \sin \varphi \cdot i))^3 = r^3 \cdot (\cos(3\varphi) + \sin(3\varphi) \cdot i)$
 - ii. $= r^3 \cdot (\cos(3\varphi + 2\pi) + \sin(3\varphi + 2\pi) \cdot i)$
 $= r^3 \cdot (\cos(3\varphi) + \sin(3\varphi) \cdot i)$
 - iii. $= 2$
 bzw. $= 2 \cdot (\cos(\frac{2\pi}{3}) + \sin(\frac{2\pi}{3}) \cdot i)$
 bzw. $= 2 \cdot (\cos(\frac{4\pi}{3}) + \sin(\frac{4\pi}{3}) \cdot i)$

[Der Radius der komplexen Wurzeln $\sqrt[3]{8}$ in Polardarstellung ist 2. Passender Winkel der komplexen Wurzeln $\sqrt[3]{8}$ ist jeder Winkel in $[0, 2\pi)$, dessen Dreifaches ein Vielfaches von 2π ist.]

5.12 Gleichmächtigkeit

- a) Reflexivität: id_M bildet M bijektiv auf M ab.
- b) Symmetrie: Ist $f : M \rightarrow N$ bijektiv, dann auch $f^{-1} : N \rightarrow M$.
- c) Transitivität: Sind $f : M \rightarrow N$ und $g : N \rightarrow O$ bijektiv, dann auch $g \circ f : M \rightarrow O$.

5.13 Gleichmächtigkeit und Abbildungen

[Natürlich folgt die Behauptung aus dem Endlichkeitskriterium in Satz 5.11, aber hier soll die Aussage „zu Fuß“, ohne 5.11, gezeigt werden.]

Wir bezeichnen die Mächtigkeit einer Menge S als $|S|$. Hier, bei endlichen Mengen, ist dies jeweils eine natürliche Zahl.

Induktionsanfang:

Die Aussage stimmt für Mengen M und N der Mächtigkeit von 0 bis 0, d.h. der Mächtigkeit 0, d.h. für $M = N = \emptyset$, denn dann ist die einzige Abbildung von M nach N die leere (d.h. die Relation zwischen M und N mit null Paaren), und die ist sowohl injektiv als auch surjektiv.

Induktionsschritt:

Die Aussage stimme für je zwei Mengen der Mächtigkeit n (Induktionsannahme \circ), und die Mächtigkeit $|M|$ bzw. $|N|$ zweier Mengen M und N sei jeweils $n+1$. Wegen $n+1 > 0$ enthält M mindestens ein Element m_0 . Sei $M' := M \setminus \{m_0\}$.

- Sei $f: M \rightarrow N$ eine injektive Abbildung. Mit $N' := N \setminus \{f(m_0)\}$ gilt für jedes $m \in M'$, dass $f(m) \in N'$, denn sonst wären $m \neq m'$ und $f(m) = f(m')$, also f nicht injektiv. Also gibt es die Abbildung $f': M' \rightarrow N'$ definiert durch $f'(m) := f(m)$ und mit $|M'| = |N'| = n$. Sie ist ebenfalls injektiv, da aus $f'(m_1) = f'(m_2)$ folgt, dass $f(m_1) = f(m_2)$, also $m_1 = m_2$ gilt. Wegen (\circ) ist sie surjektiv. Damit ist f aber auch surjektiv, denn jedes Element $y \in N$ ist entweder in N' und hat ein f' -Urbild in M' , oder es ist $y = f(m_0)$, so dass es in beiden Fällen ein f -Urbild in M hat.
- Sei nun $f: M \rightarrow N$ eine surjektive Abbildung und $f': M' \rightarrow N$ die Einschränkung von f auf $M \setminus \{m_0\}$. $f'_{\{\}}(M') = f_{\{\}}(M')$ kann höchstens so viele Elemente wie M' enthalten, nämlich für $M' = \{m_1, \dots, m_n\}$ die Elemente $f(m_1), \dots, f(m_n)$, und das sind, wenn sie alle voneinander verschieden sind, n Stück, ansonsten weniger. [Diese anschauliche Begründung wäre streng genommen auch induktiv zu beweisen.]
 $f'_{\{\}}(M') = f_{\{\}}(M')$ umfasst entweder ganz N , falls nämlich $f(m_0)$ noch ein anderes f -Urbild in M hat, oder ihm fehlt genau $f(m_0)$. Im ersten Fall wäre f' surjektiv, und es gälte

$$n+1 = |M| > |M'| \geq |f'_{\{\}}(M')| = |N| = n+1,$$

was, da man daraus auf $n+1 > n+1$ schließen kann, unmöglich ist. Im einzig möglichen zweiten Fall ist mit $N' := N \setminus \{f(m_0)\}$ durch

$$f'': \begin{cases} M' & \rightarrow & N' \\ m & \mapsto & f'(m) \end{cases}, \text{ d.h. gleichbedeutend } f'': \begin{cases} M \setminus \{m_0\} & \rightarrow & N \setminus \{f(m_0)\} \\ m & \mapsto & f(m) \end{cases},$$

eine surjektive Abbildung definiert, und die ist wegen $|M'| = |N'| = n$ und (\circ) auch injektiv. Da es sich um den Fall handelt, dass $f(m_0)$ kein weiteres f -Urbild in M hat, ist damit auch f injektiv.

5.14 Kombinatorik: Abbildungen, Inklusion-Exklusion

- a) Sei M_n die Menge der durch n teilbaren Zahlen x mit $1 \leq x \leq 10000$. Man sieht leicht: $M_n \cap M_m = M_{\text{ggT}(n,m)}$, und $|M_n|$ ist die größte natürliche Zahl x mit $n \cdot x \leq 10000$ bzw. die kleinste natürliche Zahl y mit $n \cdot (y+1) > 10000$.

Wir möchten $|M_4 \cup M_5 \cup M_6|$ ermitteln. Würden wir dafür $|M_4| + |M_5| + |M_6|$ ansetzen, so hätten wir die Zahlen, die Elemente genau zweier dieser Mengen sind, doppelt gezählt, und die Zahlen in $M_4 \cap M_5 \cap M_6 = M_{120}$ hätten wir sogar dreimal gezählt.

Subtrahieren wir zum Ausgleich die Anzahlen der Elemente von $M_4 \cap M_5 (= M_{20})$, $M_4 \cap M_6 (= M_{24})$ und $M_5 \cap M_6 (= M_{30})$, so haben wir die in allen drei Schnittmengen enthaltenen durch 4, 5 und 6 teilbaren Zahlen, also M_{120} , auch dreimal abgezogen, müssen sie also am Ende noch einmal hinzurechnen. Insgesamt folgt (wie uns auch die Siebformel verraten hätte):

$$\begin{aligned} |M_4 \cup M_5 \cup M_6| &= |M_4| + |M_5| + |M_6| - |M_{20}| - |M_{24}| - |M_{30}| + |M_{120}| \\ &= 2500 + 2000 + 1666 - 500 - 416 - 333 + 83 \\ &= 5000 \end{aligned}$$

- b) Der Einfachheit halber beschränken wir uns auf $M = \{1, \dots, m\}$ und $N = \{1, \dots, n\}$. Wir können uns ja die Elemente von M und N jeweils als a_1 bis a_m bzw. b_1 bis b_n durchnummeriert denken; dann entsprechen die Abbildungen zwischen den Mengen einander eineindeutig: Die Abbildung g mit $g(a_i) = b_k$ entspricht der Abbildung \tilde{g} mit $\tilde{g}(i) = k$. Die gesuchte Zahl nennen wir $\text{Sur}(m, n)$.

Sei $f: M \rightarrow N$. Ist $m < n$, so umfasst $f(M)$ höchstens m Bildpunkte, genauer gesagt m bei injektivem f , sonst echt weniger. Also kann f nicht surjektiv sein, da $n - m$ Elemente von N kein Urbild haben.

$$m < n \Rightarrow \text{Sur}(m, n) = 0.$$

Ist $m = n$, dann ist ein surjektives f bijektiv und entspricht genau einer Permutation auf $\{1, \dots, n\}$. Also gibt es dann $n!$ surjektive Abbildungen.

$$m = n \Rightarrow \text{Sur}(m, n) = n!.$$

Aber das erhalten wir auch als Spezialfall von $m \geq n$, was wir nun voraussetzen.

1. Lösungsweg

In der Menge N^M aller $f: M \rightarrow N$, die ja $|N|^{|M|}$ (also n^m) Elemente hat, gibt es für jedes $i = 1, \dots, n$ die Teilmenge

$$F_i := \{f: M \rightarrow N \mid i \notin f(M)\}$$

der Abbildungen, bei denen i nicht Bildpunkt ist. Jede Abbildung in F_i entspricht per Verkleinerung des Wertebereichs genau einer Abbildung $f: M \rightarrow N \setminus \{i\}$ und umgekehrt. Von diesen gibt es $(|N \setminus \{i\}|)^{|M|}$, d.h. $(n-1)^m$ verschiedene. Sind i_1, i_2, \dots, i_k unterschiedliche Zahlen aus $\{1, \dots, n\}$, so ist $F_{i_1} \cap F_{i_2} \cap \dots \cap F_{i_k}$ die Menge der Abbildungen $f: M \rightarrow N$, bei denen keine der Zahlen i_1, i_2, \dots, i_k Bildpunkt ist. Analog zum Obigen ist deren Anzahl identisch mit der Anzahl der Abbildungen von M in $N \setminus \{i_1, i_2, \dots, i_k\}$, wovon es wiederum $(n-k)^m$ verschiedene gibt.

Eine nicht surjektive Abbildung von M nach N ist eine, bei der mindestens ein $i = 1, \dots, n$ nicht Bildpunkt ist, also ein Element von $F_1 \cup F_2 \cup \dots \cup F_n$, und umgekehrt. Wir bestimmen die Mächtigkeit dieser Menge über die Siebformel (Satz 8.2):

$$|F_1 \cup F_2 \cup \dots \cup F_n| = \sum \{|F_i| \mid 1 \leq i \leq n\} - \sum \{|F_i \cap F_k| \mid 1 \leq i, k \leq n, i \neq k\} \\ + \sum \{|F_i \cap F_k \cap F_l| \mid 1 \leq i, k, l \leq n, \{i, k, l\} = 3\} - \dots$$

Die Durchschnitte aus r Mengen sind hierbei untereinander gleichmächtig, und ihre Anzahl entspricht der der r -elementigen Teilmengen von $\{1, \dots, n\}$. Also:

$$|F_1 \cup F_2 \cup \dots \cup F_n| = n \cdot (n-1)^m - \binom{n}{2} \cdot (n-2)^m + \dots + (-1)^n \binom{n}{n} \cdot (n-n)^m.$$

Diese Zahl ist von der Anzahl aller Abbildungen zu subtrahieren, damit wir als Endergebnis für die Anzahl der surjektiven Abbildungen erhalten:

$$Sur(m, n) = \sum_{k=0}^n (-1)^k \cdot \binom{n}{k} \cdot (n-k)^m = \sum_{i=0}^n (-1)^{n-i} \cdot \binom{n}{i} \cdot i^m.$$

[Wegen des Falls $m = n$ haben wir nebenbei gezeigt: $n! = \sum_{i=1}^n (-1)^{n-i} \cdot \binom{n}{i} \cdot i^n$.]

2. Lösungsweg

Jede surjektive Abbildung $f: M \rightarrow N$ liefert mit $M_k := f^{-1}(\{k\})$ für $1 \leq k \leq n$ ein n -Tupel M_1, \dots, M_n derart, dass $\{M_1, \dots, M_n\}$ eine Partition von M ist. Da wir diese mitsamt einer Reihenfolge darauf erhalten, man spricht von einer geordneten Partition, und umgekehrt jede solche geordnete Partition M_1, \dots, M_n vermittelt $x \in M_i \Rightarrow f(x) := i$ eine surjektive Abbildung definiert, gibt es genauso viele surjektive $f: M \rightarrow N$ wie geordnete Partitionen M_1, \dots, M_n von M . Da sich jede Partition $\{M_1, \dots, M_n\}$ in $n!$ unterschiedliche Reihenfolgen bringen lässt, ist $Sur(m, n)$ das n -fache der Anzahl $S_{m,n}$ möglicher n -elementiger Partitionen $\{M_1, \dots, M_n\}$ von $M = \{1, \dots, m\}$.

$$Sur(m, n) = n! \cdot S_{m,n}$$

$S_{m,n}$ nennt man Sterling-Zahlen zweiter Art. Wie lassen sich die $S_{m,n}$ rekursiv berechnen? Nur die leere Menge lässt sich durch eine leere Partition überdecken, und die leere Menge lässt sich ausschließlich durch eine leere Partition überdecken. (Die Elemente einer Partition sollen nichtleere Teilmengen von M sein, vgl. Korrekturliste zum Buch.) In Formeln:

$$S_{0,0} = 1 \text{ und } k > 1 \Rightarrow S_{0,k} = S_{k,0} = 0.$$

Mit der Rekursionsgleichung

$$S_{m+1,n} = n \cdot S_{m,n} + S_{m,n-1}$$

lassen sich dann beliebige $S_{m,n}$ und $Sur(m, n)$ berechnen. Wie begründet man diese?

Die Menge der n -elementigen Partitionen von $\{1, \dots, m+1\}$ zerfällt in zwei disjunkte Teilmengen, die Partitionen mit Element $\{m+1\}$ (Teilmenge *Mit*) und diejenigen ohne (Teilmenge *Ohne*). Jede Partition P aus *Mit* entspricht eineindeutig einer $(n-1)$ -elementigen Partition $P \setminus \{m+1\}$ auf $\{1, \dots, m\}$. Von den letzteren gibt es $S_{m,n-1}$ Stück. Wie viele Elemente hat *Ohne*? Wir denken uns jedes Partition in *Ohne* eineindeutig in zwei Schritten aufgebaut: Wir bilden eine n -elementige Partition auf $\{1, \dots, m\}$, was auf $S_{m,n}$ Weisen geht, und stecken $m+1$ zu einer der n Mengen in der Partition dazu, was auf n Weisen geht. Also hat *Ohne* $n \cdot S_{m,n}$ Elemente – was den Beweis abschließt.

5.15 Kombinatorik: Beweisbeispiele

- a) Additivität bei disjunkten Vereinigungen: Die Formel ist trivial für $n=1: |A_1| = |A_1|$. Gilt sie für n , d.h. streng paarweise geklammert, also

$$|(\dots(A_1 \cup A_2) \cup \dots \cup A_n)| = (\dots(|A_1| + |A_2|) + \dots + |A_n|),$$

so kommen bei der Vereinigung mit der zum Bisherigen disjunkten Menge A_{n+1} die $|A_{n+1}|$ neuen Elemente von A_{n+1} hinzu:

$$|((\dots(A_1 \cup A_2) \cup \dots \cup A_n) \cup A_{n+1})| = (\dots(|A_1| + |A_2|) + \dots + |A_n|) + |A_{n+1}|.$$

Wer mag, kann diesen Beweis mathematisch strenger führen, nämlich über die Existenz einer formal definierten bijektiven Abbildung $f: \sum_{i=1}^n |A_i| \rightarrow \bigcup_{i=1}^n A_i$.

- b) Wir zeigen: Wenn $\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} + \frac{n!}{(k-1)! \cdot (n-k+1)!}$

$$\begin{aligned} \binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k! \cdot (n-k)!} + \frac{n!}{(k-1)! \cdot (n-k+1)!} && \text{(per Definition bzw. Induktionsannahme)} \\ &= \frac{n! \cdot (n-k+1)}{k! \cdot (n-k)! \cdot (n-k+1)} + \frac{k \cdot n!}{k \cdot (k-1)! \cdot (n-k+1)!} && \text{(Brüche erweitert)} \\ &= \frac{(n-k+1+k) \cdot n!}{k! \cdot (n-k+1)!} && \text{(In jedem Nenner zwei Faktoren zusammengefasst und dann gleichnamige Brüche addiert)} \\ &= \frac{(n+1)!}{k! \cdot ((n+1)-k)!} && \text{(Zähler ausgerechnet)} \\ &= \binom{n+1}{k}. && \text{(per Definition)} \end{aligned}$$

- c) Wir beweisen die Aussage $\forall A [|A| = n \rightarrow \forall k \in \mathbb{N}_0 |\{B \mid B \subseteq A \wedge |B| = k\}| = 1 = \binom{n}{k}]$

mittels vollständiger Induktion für alle $n \in \mathbb{N}$.

Induktionsanfang, $n=1$:

Aus $|A| = 1$ folgt $A = \{a\}$ für ein a , und $B \subseteq A \wedge |B| = k$ gilt nur für $B = \emptyset$ und $k=0$ bzw. $\{a\}$ und $k=1$. Sowohl für $k=0$ als auch für $k=1$ ist

$$|\{B \mid B \subseteq A \wedge |B| = k\}| = 1 = \binom{|A|}{k}.$$

Induktionsschritt:

Die Aussage gelte für ein $n \in \mathbb{N}$. Wir wollen sie für $n+1$ beweisen:

Ist $A = \{a_1, \dots, a_{n+1}\}$ eine Menge mit $n+1$ Elementen, so haben wir zu zeigen dass

für alle k von 0 bis $n+1$ gilt: $|\{B \mid B \subseteq A \wedge |B| = k\}| = \binom{n+1}{k}$. Eine k -elementige

Teilmenge B von A ist nun entweder eine Teilmenge von $\{a_1, \dots, a_n\}$ oder nicht. Im

ersten Fall gibt es laut Voraussetzung $\binom{n}{k}$ unterschiedliche Möglichkeiten. Im

zweiten Fall setzt B sich zusammen aus a_{n+1} und einer $(k-1)$ -elementigen Teilmenge

von $\{a_1, \dots, a_n\}$, wofür es laut Voraussetzung $\binom{n}{k-1}$ unterschiedliche Möglichkeiten

gibt. Die Mengen der B gemäß den beiden Fällen sind disjunkt, da die letzteren a_{n+1}

enthalten und die anderen nicht, so dass sich gemäß (a) ihre Anzahlen addieren. Also ist die Gesamtzahl der Möglichkeiten

$$\binom{n}{k} + \binom{n}{k-1}, \text{ d.h. nach (b): } \binom{n+1}{k}.$$

- d) Schauen Sie z.B. nach bei <http://www.goldennumber.net/pascals-triangle/> oder <http://milan.milanovic.org/math/english/fibo/fibo4.html>, sowie in Wikipedia unter Fibonacci und Catalan.

Beispielsweise ist die Summe der Zahlen der n -ten Zeile des Pascal'schen Dreiecks die n -te Zweierpotenz, d.h. formal geschrieben $\sum_{k=0}^n \binom{n}{k} = 2^n$, und dies leuchtet leicht ein:

- Wegen $\binom{0}{0} = 1 = 2^0$ gilt es für die 0-te Zeile (die Spitze) des Dreiecks.
- Da jede Zahl in der $n+1$ -ten Zeile des Dreiecks die Summe der linken und rechten oberen Nachbarin ist, gehen die Zahlen der darüberliegenden n -ten Zeile alle zweimal in die Summe der $n+1$ -ten Zeile ein, so dass die Summe über die $n+1$ -te Zeile das Doppelte der Summe über die n -ten Zeile ergibt.

am Rand:
$$\begin{array}{c} \binom{0}{0} \quad 1 \\ \diagdown \quad \diagup \\ + \\ | \\ 1 \end{array}$$

innen:
$$\begin{array}{c} \binom{n}{k-1} \quad \binom{n}{k} \\ \diagdown \quad \diagup \\ + \\ | \\ \binom{n+1}{k} \end{array}$$

[Unter Verwendung der Binomialexpansion, angewendet auf $(1+1)^n$, geht das Ganze sogar noch kürzer.]

5.16 Kombinatorik: Kugeln in Urnen

- a) [Vergleiche Übersicht in Tab. 5.2!]

Geordnet, mit Zurücklegen: $n^k = 7^4 = 7 \cdot 7 \cdot 7 \cdot 7 = 2401$.

[Mit Kugeln 1 bis 7: 1111, 1112, ..., 1117, 1121, 1122 usw. bis 7777, den Zeichenfolgen der Länge 4 über $\{1, \dots, 7\}$ entsprechend.]

Geordnet, ohne Zurücklegen: $n!/(n-k)! = 7!/(7-4)! = 7 \cdot 6 \cdot 5 \cdot 4 = 840$.

[Mit Kugeln 1 bis 7: 1234, 1243, 1324, usw. bis 7654, den Permutationen von jeweils 4 aus $\{1, \dots, 7\}$ entsprechend.]

Ungeordnet, ohne Zurücklegen: $C(n, k) = \binom{7}{4} = \frac{7!}{4! \cdot 3!} = \frac{7 \cdot 6 \cdot 5 \cdot 4}{4 \cdot 3 \cdot 2 \cdot 1} = 35$.

[Mit Kugeln 1 bis 7: $\{1, 2, 3, 4\}$, $\{1, 2, 3, 5\}$, $\{1, 2, 3, 6\}$, usw. bis $\{4, 5, 6, 7\}$, den 4-elementigen Teilmengen von 1 bis 7 entsprechend.]

Ungeordnet, mit Zurücklegen: $\binom{n+k-1}{k} = \binom{10}{4} = \frac{10!}{4! \cdot 6!} = \frac{10 \cdot 9 \cdot 8 \cdot 7}{4 \cdot 3 \cdot 2 \cdot 1} = 35$.

[Mit Kugeln 1 bis 7: $\{1, 1, 1, 1\}_\mu$, $\{1, 1, 1, 2\}_\mu$, $\{1, 1, 1, 3\}_\mu$, usw. bis $\{7, 7, 7, 7\}_\mu$, den 4-elementigen Multimengen über 1 bis 7 entsprechend.]

- b) *Geordnet, mit Zurücklegen:* $n^k = 2^4 = 2 \cdot 2 \cdot 2 \cdot 2 = 16$
 $n = 2$, da nur Ergebnisse r oder s möglich.
 Mit Kugelvorrat $\{r, r, r, r, s, s, s\}_\mu$: $rrrr, rrrs, rrsr, rrss$, usw. bis $sssr, ssss$
Geordnet, ohne Zurücklegen: wie vorher, aber ohne $ssss$, also 15.
 Mit Kugelvorrat $\{r, r, r, r, s, s, s\}_\mu$: $rrrr, rrrs, rrsr, rrss$, usw. bis $sssr$
Ungeordnet, ohne Zurücklegen: 4.
 Mit Kugelvorrat $\{r, r, r, r, s, s, s\}_\mu$: $\{r, r, r, r\}_\mu, \{r, r, r, s\}_\mu, \{r, r, s, s\}_\mu, \{r, s, s, s\}_\mu$
Ungeordnet, mit Zurücklegen: 5
 Nämlich wie ohne Zurücklegen plus die Möglichkeit $\{s, s, s, s\}_\mu$

[Dämpfer: Reine Zählungen wie in (b) haben meist geringe Bedeutung, da in der Wahrscheinlichkeitsrechnung die einzelnen Stichproben danach zu gewichten sind, auf wieviele unterschiedliche Arten (mit unterschiedlichen Kugeln) sie zustande kommen können.]

5.17 Kombinatorik: Wege und Wörter

- a) Bewegungsrichtungen A(bwärts) und R(echts).
 Wegbeschreibungen: Folgen aus n R's und m A's, im Beispiel also RRARA und AARRR. Alle diese sind Permutationen einer als Folge notierten Multimenge (sog. Permutationen einer Multimenge), wovon es

$$(m+n)!/(m! \cdot n!)$$
 verschiedene gibt.

[Schaut man auf die Positionen der m A's als Teilmengen von $\{1, 2, \dots, m+n\}$, so erweist sich dies (natürlich) gleichzeitig als Anzahl der m -elementigen (aber auch der n -elementigen) Teilmengen einer $(m+n)$ -elementigen Menge: $\binom{m+n}{m} = \binom{m+n}{n}$.]

- b) Auch dies ist ein Fall von Permutationen einer Multimenge, hier also
 $(11)!/(4! \cdot 4! \cdot 2! \cdot 1!) = (11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4!)/(4! \cdot (4 \cdot 2) \cdot (3 \cdot 2)) = 11 \cdot 10 \cdot 9 \cdot 7 \cdot 5 = 34.650$.
- c) Erste Frage: Für das erste A gibt es drei Möglichkeiten, dann für das erste N zwei, für das zweite N eine und für das zweite A noch zwei, zusammen genommen $3 \cdot 2 \cdot 1 \cdot 2 = 12$.

Zweite Frage: ... und dies unter $7 \cdot 6 \cdot 5 \cdot 4 = 840$ gleichberechtigten möglichen Stichproben. Wie am Ende der Lösung von 5.14 angedeutet, ist eine solche Fragestellung ein Schritt hin zur Wahrscheinlichkeitsberechnung: Die Chance, ANNA zu ziehen, ist $12/840$.

5.18 Kombinatorik: Multimengen und Folgen

- Man schreibt alle 1024 zehngliedrigen Folgen aus Einsen und Nullen auf – systematisch, ohne eine zu vergessen oder mehrfach aufzuschreiben. Beispielsweise kann man alle Binärzahlen von 1024 bis 2047 in wachsender Größe schreiben und überall die führende Eins weglassen (bzw. die von 0 bis 1023, aber vorne mit Nullen auf zehn Zeichen aufgefüllt). Dann zählt man unter den aufgeschriebenen Folgen diejenigen mit genau 6 Einsen.

- Man kann sich aber auch das Aufschreiben der unpassenden Zahlen ersparen, indem man gleich systematisch nur alle Folgen aus 6 Einsen und 4 Nullen generiert (und sie dann zählt), etwa mit der Deklaration:

```
DoIt(i,k,string) :=
BEGIN
  IF i=0 AND k=0 THEN BEGIN PRINT("-"); PRINT(string) END;
  IF i>0 THEN DoIt(i-1,k,attach(string,'1'));
  IF k>0 THEN DoIt(i,k-1,attach(string,'0'));
END
```

und deren Aufruf mit `DoIt(6,4,"")`.

- Man definiert und berechnet unmittelbar die Funktion $Anz(i,k)$ der Anzahl aller Folgen aus i Einsen und k Nullen ($i,k \geq 0$) rekursiv, indem man (abgesehen von den Randfällen) zwischen den mit 1 beginnenden und den mit 0 beginnenden unterscheidet:

```
Anz(i,k) := IF (i=0 OR k=0) THEN 1
              ELSE Anz(i-1,k) + Anz(i,k-1)
```

Damit ruft man auf: `Anz(6,4)`.

- Man kann die Folgen eindeutig codieren durch die Angabe der vier Positionen der Nullen in der Folge. Die gesuchte Anzahl ist also auch die Anzahl der vier-elementigen Teilmengen der zehn-elementigen Menge $\{1, \dots, 10\}$, und das sind alle ungeordneten 4-aus-10-Stichproben ohne Zurücklegen, also $C(10,4) = \binom{10}{4} = 210$.

- Analog könnte man den 6 Einsen ihre Positionen zuordnen und gelangt so zu $C(10,6)$, was den gleichen Wert ergibt.
- Wenn man die Einsen als Trennstriche zwischen den Nullen auffasst, so dass sich die Nullen auf die 7 Bereiche vor, zwischen und hinter den Trennstrichen verteilen, kann man die gesuchten 0-1-Folgen auch als *Verteilungsergebnisse* sehen. Man stellt sich vor, dass man vier ununterscheidbare Kugeln auf sieben unterscheidbare Urnen 1 bis 7 verteilt (Modell A). Nun entspricht das Legen einer Kugel in Urne i in Modell A dem Ziehen der Kugel i aus einer Urne mit Kugeln 1 bis 7 und anschließendem Zurücklegen (Modell B). Das Zurücklegen rührt daher, dass in Modell A die Urne i auch für weitere Kugeln zur Verfügung steht. Dass in Modell A die Kugeln ununterscheidbar sind, bedeutet in Modell B, dass nicht die genaue Folge der gezogenen Kugelnummern als Ergebnis zählt sondern wie oft jede vorkommt, also deren Multimenge. Die *Verteilungsergebnisse* entsprechen also *Ziehungsergebnissen*, nämlich den ungeordneten 4-aus-7-Stichproben mit Zurücklegen, mit der Anzahl

$$\binom{7+4-1}{4} = C(10,4) = \binom{10}{4} = 210.$$

- Analog könnte man vier die Nullen als Trennzeichen von fünf Bereichen betrachten und nach der obigen Überlegung fragen: Wie oft hat man jede von fünf unterscheidbaren Kugeln 1 bis 5 gezogen, wenn man sechsmal zieht und zurücklegt? Das führt analog zu $\binom{5+6-1}{6} = \binom{10}{6} = 210$.

5.19 Kombinatorik: Abbildungen

Wie kann man im Falle $M = \{a_1, a_2, \dots, a_{m-1}, a_m\}$ und $|N| = n$ eine injektive Abbildung $f : M \rightarrow N$ bestimmen? Zuerst kann man $f(a_1)$ unter den n Elementen von N frei wählen, dann – um die Injektivität zu wahren – $f(a_2)$ unter den $n-1$ Elementen von $N \setminus \{a_1\}$, $f(a_3)$ unter den $n-2$ Elementen von $N \setminus \{f(a_1), f(a_2)\}$, usw. Nach dem Prinzip der Verkettung von (hier nacheinander m) Auswahlmöglichkeiten gibt es daher

$$(n-0) \cdot (n-1) \cdot (n-2) \cdot \dots \cdot (n-(m-1)) = \frac{n!}{(n-m)!}$$

injektive Abbildungen $f : M \rightarrow N$. Dies gilt natürlich nur, wenn $m \leq n$, denn sonst gibt es dabei mittendrin kein einziges Element mehr zum Auswählen, also auch keine einzige injektive Abbildung, so dass deren Anzahl dann 0 beträgt.

[Wer mag, kann sich dieses noch recht formlos erlangte Ergebnis etwas formaler beweisen, etwa nach folgendem Schema:

- Man leitet zum einen aus $f : M \rightarrow N$ injektiv $\wedge |M| = m \wedge |N| = n \wedge m > n$ einen Widerspruch ab, was dann die oben abschließend erwähnte Anzahl 0 beweist.
- Dann beweist man für beliebiges $k \geq 0$ die Aussage

$$(|M| = m \wedge |N| = m+k) \Rightarrow |\{f : M \rightarrow N \mid f \text{ injektiv}\}| = \frac{(m+k)!}{k!}$$

induktiv für alle $m \geq 0$, denn:

- Sie gilt für $m=0$ (wegen der leeren als einziger injektiver Abbildung).
- Wenn sie für m gilt (#), so gilt sie auch für $m+1$ anstelle von m , denn es gibt dann ein $a \in M$ und bei injektivem $f : M \rightarrow N$ daher $m+k+1$ Möglichkeiten für $f(a)$ und wegen (#) $m+k/k!$ Möglichkeiten für die – dann auch wohldefinierte und injektive – Abbildung $g : M \setminus \{a\} \rightarrow N \setminus \{f(a)\}$ mit $g(x) := f(x)$.

Wem das noch nicht reicht, der kann auch den Multiplikationseffekt bei verketteten Wahlmöglichkeiten über eine Betrachtung der Mächtigkeit geeigneter kartesischer Produkte formal beweisen.]

5.20 Unendliche Anzahlen und Hilberts Hotel

Alle bisherigen Gäste (außer dem in Zimmer 1) ziehen gleichzeitig um, und zwar aus Zimmer Nummer n in das Zimmer Nummer $2 \cdot n - 1$. Jeder neue Gast G_n bekommt das frei werdende Zimmer Nummer $2 \cdot n$.

[Oder auch umgekehrt, alle alten Gäste nach $2 \cdot n$, die neuen nach $2 \cdot n - 1$.]

5.21 Einige abzählbare Mengen

- $f : n \mapsto n-1$ bildet \mathbb{N} bijektiv auf \mathbb{N}_0 und $g : n \mapsto 2n$ \mathbb{N}_0 bijektiv auf die Menge der geraden Zahlen ≥ 0 ab. Damit ist $g \circ f$ eine Bijektion von den natürlichen auf die geraden Zahlen ≥ 0 , die Mengen sind gleichmächtig, also die letztere auch abzählbar.
- h mit $h(n) := (n-1)/2$ für ungerade n und $h(n) := -(n/2)$ für gerade n bildet \mathbb{N} bijektiv auf die ganzen Zahlen ab. Damit ist h eine Bijektion von den natürlichen auf die ganzen Zahlen, die Mengen sind gleichmächtig, und die letztere ist abzählbar.

- c) Ist A abzählbar unendlich (wegen der Verkettung von Bijektionen genügt hier der Fall $A = \mathbb{N}$) und $M \subseteq A$ unendlich, dann betrachten wir die Abbildung $f: \mathbb{N} \rightarrow M$, die wie folgt induktiv definiert ist (und quasi M nach wachsender Größe ordnet):

$$f(1) := \min M, \quad f(n+1) := \min (M \setminus \{f(1), \dots, f(n)\}).$$

Sie ist injektiv, sonst wäre mit $f(n) = f(m)$, $n > m$, $f(n)$ das Minimum und damit Element einer Menge, die gar nicht $f(n)$ enthält. Zu jedem $m \in M$ existieren nur endlich viele, nämlich höchstens $n-1$ kleinere Elemente in M , sagen wir i Stück. Dann ist $m = f(i+1)$. Also ist f auch surjektiv und insgesamt eine Bijektion von \mathbb{N} auf M , und somit M abzählbar.

- d) Die Abbildung $f: \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ mit $f(n) := (n, 1)$ ist eine injektive Abbildung, woraus nach Satz 5.7 über die Eigenschaften der Mächtigkeitsrelationen $\mathbb{N} \preceq \mathbb{N} \times \mathbb{N}$ folgt. Nach Satz 5.21, dem Fundamentalsatz der Arithmetik ist $g: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ mit $g(m, n) := 2^m \cdot 3^n$ injektiv, woraus nach Satz 5.7 $\mathbb{N} \times \mathbb{N} \preceq \mathbb{N}$ folgt. Satz 5.13 von Schröder, Bernstein und Cantor liefert mit $\mathbb{N} \sim \mathbb{N} \times \mathbb{N}$ die gewünschte Abzählbarkeit. [Abbildung 5.18 liefert eine anschauliche weitere Beweisidee.]

- e) Die Folgenmenge bezeichnen wir mit F , die n -te Primzahl als p_n . Der Beweis der Abzählbarkeit von F entspricht dem Beweis in (d), wobei in analogen Rollen die Funktionen

$$f: \begin{cases} \mathbb{N} & \rightarrow & F \\ n & \mapsto & (n) \end{cases} \quad \text{und} \quad g: \begin{cases} F & \rightarrow & \mathbb{N} \\ (x_1, x_2, \dots, x_n) & \mapsto & 2^{x_1} \cdot 3^{x_2} \cdot \dots \cdot p_n^{x_n} \end{cases}$$

verwendet werden. Die Technik mit den Primzahlpotenzen bei g nennt man Gödel-Nummerierung oder Gödelisierung.

- f) Diese abzählbar vielen Mengen seien aufgezählt als M_1, M_2, \dots , mit jeweils der Mächtigkeit $m_1, m_2, \dots \in \mathbb{N}$, und wir setzen $M = \bigcup_{i=1}^{\infty} M_i$. Die endlich vielen Elemente jedes einzelnen M_i seien durchnummeriert als $x_{i,1}, x_{i,2}, \dots, x_{i,m_i}$. Da es sich um eine unendliche Menge von Mengen handelt, müssen die M_i insgesamt unendlich viele verschiedene Elemente enthalten, sonst könnte es nur endlich viele unterschiedliche M_i geben.

Für jedes $x \in M$ existiert ein kleinstes i , für das $x \in M_i$ ist – nennen wir es $r(x)$ [eine legere Funktionsdefinition]. Die eindeutige laufende Nummer von x in $M_{r(x)}$ nennen wir $s(x)$ [noch eine legere Funktionsdefinition], so dass $x = x_{r(x), s(x)}$. Die Abbildung $f: x \mapsto (r(x), s(x))$ ist injektiv von M in $\mathbb{N} \times \mathbb{N}$, so dass $M \preceq \mathbb{N} \times \mathbb{N}$. Wenn wir den Wertebereich auf $f(M)$ einschränken zur Abbildung f' , erhalten wir eine Bijektion zwischen M und $f(M)$. Letzteres ist nach (c) oben abzählbar, d.h. Bildmenge einer Bijektion g von \mathbb{N} aus. Insgesamt ist $f'^{-1} \circ g$ bijektiv von \mathbb{N} auf M , also M abzählbar.

5.22 Cantor'sches Diagonalverfahren

f ist surjektiv, denn jede Folge $x = x_1 x_2 x_3 \dots$ ist identisch mit $f(\{n \in \mathbb{N} \mid x_n = 1\})$.

f ist injektiv, denn immer wenn $f(M) = f(N) = x_1 x_2 x_3 \dots$ gilt, gilt für alle natürlichen Zahlen n : $n \in M \Leftrightarrow x_n = 1 \Leftrightarrow n \in N$, insgesamt also $M = N$.

Wären die Teilmengen abzählbar unendlich viele, M_1, M_2, \dots , könnten wir ihre zugehörigen 0-1-Folgen $f(M_n)$ wieder à la Cantor untereinander schreiben und per Diagonalverfahren eine noch nicht aufgezählte Folge bzw. zugehörige Teilmenge wie folgt konstruieren:

$$m_n = \begin{cases} 0 & \text{wenn } f(M_n)_n = 1 \\ 1 & \text{wenn } f(M_n)_n = 0 \end{cases},$$

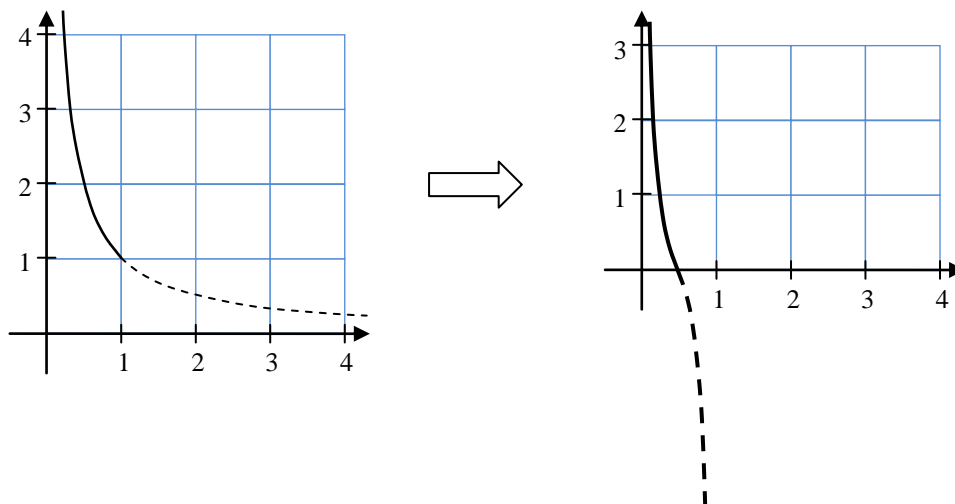
$m_1 m_2 m_3 \dots$ ist nämlich eine Folge, die nicht in der Liste $f(M_1), f(M_2), \dots$ steht, da sie sich vom n -ten Listenelement an der n -ten Stelle unterscheidet. Das f -Urbild dieser Folge wäre dann nicht unter den M_1, M_2, \dots – im Widerspruch zur Annahme, die daher nicht gelten kann.

5.23 Bijektion zwischen (0,1) und \mathbb{R}

Eine Möglichkeit: Der durchgezogene Hyperbelteil, also das Bild von $f(x) = 1/x$, $0 < x \leq 1$, wird um 1 nach unten verschoben ($f_1(x) = 1/x - 1$) und um die Hälfte in Richtung y -Achse

zusammengedrückt (also x verdoppelt): $f_2(x) = \frac{1}{2x} - 1$ (fetter Kurventeil rechts). Schließlich

wird eine Kopie des Zweiges um 180° um den Punkt $(1/2, 0)$ rotiert und angehängt (gestrichelter Kurventeil rechts). Die Rotation entspricht einer Spiegelung an der Geraden $x = 1/2$ (x durch $1-x$ ersetzen) mit anschließender Spiegelung an der x -Achse (Vorzeichenumkehr des Funktionswertes)



Insgesamt leistet daher die folgende Funktion das Gewünschte:

$$g(x) = \begin{cases} \frac{1}{2x} - 1 & , \text{ wenn } 0 < x \leq \frac{1}{2} \\ 1 - \frac{1}{2(1-x)} & , \text{ wenn } \frac{1}{2} \leq x < 1 \end{cases}$$

5.24 Gleichheit modulo als Kongruenz

Gilt $l_1 \sim_n l_2$ und $m_1 \sim_n m_2$ so existieren ganze Zahlen a und b mit $l_1 - l_2 = a \cdot n$ und $m_1 - m_2 = b \cdot n$. Also gilt ...

- bezüglich der Addition:

$$(l_1 + m_1) - (l_2 + m_2) = (l_1 - l_2) + (m_1 - m_2) = (a + b) \cdot n$$

d.h. $(l_1 + m_1) \sim_n (l_2 + m_2)$;

- bezüglich der Multiplikation:

$$\begin{aligned} l_1 \cdot m_1 - l_2 \cdot m_2 &= l_1 \cdot m_1 - l_2 \cdot m_1 + l_2 \cdot m_1 - l_2 \cdot m_2 \\ &= m_1 \cdot (l_1 - l_2) + l_2 \cdot (m_1 - m_2) \\ &= (m_1 \cdot a + l_2 \cdot b) \cdot n \end{aligned}$$

d.h. $(l_1 \cdot m_1) \sim_n (l_2 \cdot m_2)$.

5.25 Neunerprobe

Man könnte halbformal argumentieren: So wie $1000-1 = 999$, ist allgemein

$$(\#) \quad 10^k - 1 = \sum_{i=0}^{k-1} 9 \cdot 10^i.$$

Daraus folgt für die Differenz $\Delta := (n\text{-stellige Zahl } a_k a_{k-1} \dots a_1 a_0) - (\text{deren Quersumme})$:

$$\begin{aligned} \Delta &= \sum_{k=0}^n a_k \cdot 10^k - \sum_{k=0}^n a_k \\ &= \sum_{k=0}^n a_k \cdot (10^k - 1) \\ &= \sum_{k=0}^n a_k \cdot \sum_{i=0}^{k-1} 9 \cdot 10^i \\ &= 9 \cdot \left(\sum_{k=0}^n a_k \cdot \sum_{i=0}^{k-1} 10^i \right), \end{aligned}$$

sodass diese durch 9 teilbar ist. Damit sind Zahl und Quersumme immer beide durch 9 teilbar oder beide nicht.

Nun ist (#) zwar einleuchtend, aber wie könnte man „zahlentheoretisch“ argumentieren? – Wegen der Kongruenzeigenschaft von \sim_9 bezüglich der Multiplikation, siehe Satz 5.17, folgt (mit vollständiger Induktion), dass auch die gleichen Potenzen äquivalenter Zahlen äquivalent sind, so dass aus $10 \sim_9 1$ für beliebige $k > 1$ folgt: $10^k \sim_9 1$. Und ebenfalls mit Satz 5.17 folgt, dass (#') $\sum_{k=0}^n a_k \cdot 10^k \sim_9 \sum_{k=0}^n a_k \cdot 1$, und damit „ n -stellige Zahl \sim_9 Quersumme“.

[Weiterführende Anregung: Eine „Siebenerprobe“ gilt nicht, denn z.B. ist 14 durch 7 teilbar, nicht aber die Quersumme 5 von 14. „Wo“ gilt die Siebenerprobe dennoch? Tipp: am ehesten doch „dort, wo $100 - 1 = 99$ gilt“!]

5.26 Rechenregeln in Restklassenringen

Wir verzichten hier auf die vereinfachte Notation der Restklassen. Alle Eigenschaften folgen sofort aus der Definition der Rechenoperationen in \mathbb{Z}_n und den entsprechenden Eigenschaften in \mathbb{Z} (zeilenweise zu lesen):

$$\begin{aligned} [k]_{\sim_n} + [l]_{\sim_n} &= [k + l]_{\sim_n} &= [l + k]_{\sim_n} &= [l]_{\sim_n} + [k]_{\sim_n}, \\ [k]_{\sim_n} + [-k]_{\sim_n} &= [k + (-k)]_{\sim_n} &= [0]_{\sim_n}, \\ [-k]_{\sim_n} + [k]_{\sim_n} &= [(-k) + k]_{\sim_n} &= [0]_{\sim_n}, \\ [k]_{\sim_n} + ([l]_{\sim_n} + [m]_{\sim_n}) &= [k]_{\sim_n} + [l + m]_{\sim_n} &= [k + (l + m)]_{\sim_n} &= [(k + l) + m]_{\sim_n} \\ &= [k + l]_{\sim_n} + [m]_{\sim_n} &= ([k]_{\sim_n} + [l]_{\sim_n}) + [m]_{\sim_n} \\ [k]_{\sim_n} \cdot ([l]_{\sim_n} + [m]_{\sim_n}) &= [k]_{\sim_n} \cdot [l + m]_{\sim_n} &= [k \cdot (l + m)]_{\sim_n} &= [k \cdot l + k \cdot m]_{\sim_n} \\ &= [k \cdot l]_{\sim_n} + [k \cdot m]_{\sim_n} &= ([k]_{\sim_n} \cdot [l]_{\sim_n}) + ([k]_{\sim_n} \cdot [m]_{\sim_n}) \end{aligned}$$

5.27 Rechen- und Mengenoperationen auf Restklassen

a) Wir müssen hier zwischen Restklassen und Zahlen unterscheiden und verzichten daher auf die vereinfachte Notation.

- $[l]_{\sim n} + [m]_{\sim n} \subseteq \{x + y \mid x \in [l]_{\sim n} \wedge y \in [m]_{\sim n}\}$:
Für $z \in [l]_{\sim n} + [m]_{\sim n}$ gilt per Definition $z \in [l + m]_{\sim n}$, d.h. $z = l + m + t \cdot n$, also $z = (l + t \cdot n) + (m + 0 \cdot n)$.
 $x := l + t \cdot n$, $y := m + 0 \cdot n$ zeigt $z \in \{x + y \mid x \in [l]_{\sim n} \wedge y \in [m]_{\sim n}\}$.
- $\{x + y \mid x \in [l]_{\sim n} \wedge y \in [m]_{\sim n}\} \subseteq [l]_{\sim n} + [m]_{\sim n}$:
Für $z \in \{x + y \mid x \in [l]_{\sim n} \wedge y \in [m]_{\sim n}\}$ ist $z = (l + s \cdot n) + (m + t \cdot n)$, also $z = l + m + (s + t) \cdot n$, also $z \in [l + m]_{\sim n}$.

b) Nein: Wenn z.B. $n = 4$ und $l = m = 2$, dann ist $0 \in [0]_{\sim n} = [l]_{\sim n} \cdot [m]_{\sim n} \setminus \{x \cdot y \mid x \in [l]_{\sim n} \wedge y \in [m]_{\sim n}\}$, da die Beträge jedes der Produkte aus der hinteren Menge ≥ 4 sind.

5.28 Eine Folge teilerfremder Zahlen

In Übung 3.22(e) wurde gezeigt, dass $F_0 \cdot F_1 \cdot \dots \cdot F_{n-1} + 2 = F_n$, wobei $F_i = 2^{(2^i)} + 1$, d.h. insbesondere $F_0 = 2^{(2^0)} + 1 = 2^1 + 1 = 3$ gilt. Nehmen wir an, F_m und F_n mit $m < n$ hätten einen Teiler $t > 1$ gemeinsam, so wäre t auch Teiler von

$$F_n - F_m \cdot (F_0 \cdot F_1 \cdot \dots \cdot F_{m-1} \cdot F_{m+1} \cdot \dots \cdot F_{n-1}) = 2,$$

was zu $t = 2$ führt. Nun ist 2 aber weder Teiler von F_m noch von F_n , da alle Fermat-Zahlen aufgrund ihrer Definition ungerade sind. Wegen dieses Widerspruchs ist die Annahme falsch, und F_m und F_n sind teilerfremd.

5.29 Teilerfremde Multiplikatoren in Restklassenringen

Mit Übung 5.13 beispielsweise sehen wir, dass f genau dann bijektiv ist, wenn es injektiv ist. Wir zeigen in zwei Schritten, dass f genau dann injektiv ist, wenn m und n teilerfremd sind.

- Sind m und n teilerfremd, dann ist f injektiv:
Seien m und n teilerfremd, also $\text{ggT}(m, n) = 1$, und $f(i) = f(k)$, also $[m \cdot i]_{\sim n} = [m \cdot k]_{\sim n}$ bzw. $m \cdot i \sim_n m \cdot k$. Mit Lemma 5.23(a) folgt $i \sim_n k$, also $i = [i]_{\sim n} = [k]_{\sim n} = k$. Somit ist f injektiv.
- Sind m und n nicht teilerfremd, dann ist f nicht injektiv:
Sind m und n nicht teilerfremd und $a := \text{ggT}(m, n)$, so ist $a > 0$ und es existieren natürliche Zahlen b und c mit $m = a \cdot b$, $n = b \cdot c$ und $n > c > b$. Dann ist aber $f([c]_{\sim n}) = [m \cdot c]_{\sim n} = [a \cdot b \cdot c]_{\sim n} = [a \cdot n]_{\sim n} = [0]_{\sim n} = [m \cdot 0]_{\sim n} = f([0]_{\sim n})$ und f nicht injektiv.

5.30 Der größte gemeinsame Teiler als Linearkombination

a) ggT-Berechnung: $102 = 3 \cdot 30 + 12$, $30 = 2 \cdot 12 + 6$, $12 = 2 \cdot 6 + 0$.

also: $\text{ggT}(102, 30) = 6$

Rückrechnung: $12 = 102 - 3 \cdot 30$,
 $6 = 30 - 2 \cdot 12 = 30 - 2 \cdot (102 - 3 \cdot 30)$
 $= 7 \cdot 30 - 2 \cdot 102$

- b) [Der ggT mehrerer Zahlen kann, wie im Text erwähnt, durch mehrere Berechnungen eines ggT zweier Zahlen ermittelt werden, und dies in unterschiedlichen Reihenfolgen, beispielsweise

$$\text{ggT}(a, b, c) = \text{ggT}(a, \text{ggT}(b, c)) = \text{ggT}(b, \text{ggT}(a, c)) = \text{ggT}(c, \text{ggT}(a, b)).$$

Entsprechend erhält man jeweils eine Darstellung der einzelnen (End- und Zwischen-) ggTs als Linearkombination der Ausgangszahlen. Wir versuchen dies und sind am Ziel, wenn sich so *unterschiedliche* Linearkombinationen ergeben:]

$$\text{ggT}(60, 84, 210) = \text{ggT}(\text{ggT}(60, 84), 210)$$

ggT-Berechnung 60,84: $84 = 1 \cdot 60 + 24$, $60 = 2 \cdot 24 + 12$, $24 = 2 \cdot 12 + 0$.

$$\text{ggT}(60, 84) = 12$$

ggT-Berechnung 210,12: $210 = 17 \cdot 12 + 6$, $12 = 2 \cdot 6 + 0$.

$$\text{ggT}(60, 84, 210) = 6$$

Rückrechnungen: $24 = 84 - 60$, $12 = 60 - 2 \cdot 24 = 60 - 2 \cdot (84 - 60) = 3 \cdot 60 - 2 \cdot 84$,
 $6 = 210 - 17 \cdot 12 = 210 - 17 \cdot (3 \cdot 60 - 2 \cdot 84)$
 $= 210 - 51 \cdot 60 + 34 \cdot 84$

$$\text{ggT}(60, 84, 210) = \text{ggT}(\text{ggT}(60, 210), 84)$$

ggT-Berechnung 60,210: $210 = 3 \cdot 60 + 30$, $60 = 2 \cdot 30 + 0$.

$$\text{ggT}(60, 210) = 30$$

ggT-Berechnung 84,30: $84 = 2 \cdot 30 + 24$, $30 = 24 + 6$, $24 = 4 \cdot 6 + 0$.

$$\text{ggT}(60, 84, 210) = 6$$

Rückrechnungen: $30 = 210 - 3 \cdot 60$,

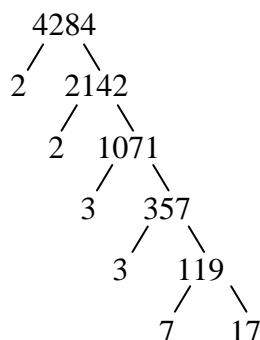
$$6 = 30 - 24 = 30 - (84 - 2 \cdot 30) = 3 \cdot 30 - 84 = 3 \cdot (210 - 3 \cdot 60) - 84$$

$$= 3 \cdot 210 - 9 \cdot 60 - 84$$

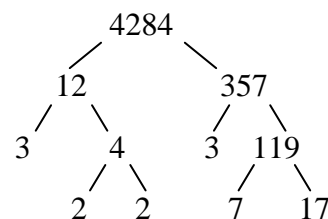
5.31 Primfaktorzerlegung

[Man kann systematisch versuchen, die Zahl (und dann die verbleibenden Quotienten) durch möglichst kleine Primfaktoren zu dividieren. Ebenso gut kann man aber auch zwischendurch in zwei Nicht-Primzahlen zu zerlegen.]

Teilerbaum systematisch



Teilerbaum alternativ



5.32 Divisionsreste

- a) Reste: 5, 0, 4, 8, 3, 7, 2, 6, 1
- b) Das sind genau alle ganzen Zahlen von 0 bis 9 – 1 wegen Lemma 5.23(c)

5.33 Multiplikativität der Euler'schen Phi-Funktion

Sind m und n teilerfremd, so haben sie keine Primfaktoren gemeinsam, die ja sonst gemeinsame Teiler wären. Hat m die Primfaktorenmenge $\{p_1, p_2, \dots, p_i\}$ und n die Primfaktorenmenge $\{q_1, q_2, \dots, q_k\}$ – hier ist also jede in der Primfaktorzerlegung mehrfach vorkommende Primzahl nur einmal aufgezählt –, so hat $m \cdot n$ die Primfaktorenmenge

$$\begin{aligned} \{p_1, p_2, \dots, p_i, q_1, q_2, \dots, q_k\}, \text{ und} \\ \varphi(m \cdot n) &= m \cdot n \cdot (1 - 1/p_1) \cdot \dots \cdot (1 - 1/p_i) \cdot (1 - 1/q_1) \cdot \dots \cdot (1 - 1/q_k) \\ &= m \cdot (1 - 1/p_1) \cdot \dots \cdot (1 - 1/p_i) \cdot n \cdot (1 - 1/q_1) \cdot \dots \cdot (1 - 1/q_k) \\ &= \varphi(m) \cdot \varphi(n) \end{aligned}$$

5.34 Satz von Euler

11 und 8 sind teilerfremd, $\text{ggT}(11, 8) = 1$.

$$\varphi(8) = |\{1, 3, 5, 7\}| = 4$$

Eulers Verallgemeinerung des Fermat'schen Satzes $\Rightarrow 11^4 \equiv 1 \pmod{8}$,
und damit gilt modulo 8:

$$\begin{aligned} 11^4 &\equiv 1 \text{ sowie } 11 \equiv 3 \text{ und infolgedessen} \\ 11^{111} &\equiv 11^{4 \cdot 27 + 3} \equiv (11^4)^{27} \cdot 11^3 \equiv 1^{27} \cdot 3^3 \equiv 27 \equiv 3. \end{aligned}$$

5.35 Eindeutige Division im Restklassenring

$[7 \cdot x \equiv 24 \pmod{30}]$ lautet in anderer Notation $7 \cdot x \sim_{30} 24$ bzw. $[7]_{\sim_{30}} \cdot [x]_{\sim_{30}} = [24]_{\sim_{30}}$

Wegen $7 \cdot x = 24 + z \cdot 30$ für ein $z \in \mathbb{Z}$ muss auch die linke Seite $7 \cdot x$, und damit x , durch 6 teilbar sein: $x = 6 \cdot x'$ für ganzzahliges x' .

Mit $m := 6$, $n := 30$, $i := 7 \cdot x'$ und $k := 24 + 5 \cdot z$ liefert das Obige:

$$m \cdot i \sim_n m \cdot k \text{ und } \text{ggT}(m, n) = 6,$$

und gemäß Lemma 5.23(1) folgt daraus $7 \cdot x' \sim_5 4 + 5 \cdot z \sim_5 4$.

Versuche, die letzte Kongruenz mit $x' = 1, 2, 3, \dots$ zu erfüllen, liefern $x' = 2$, $x = 12$ und $7 \cdot x = 24 + z \cdot 30$ mit $z = 2$, also $7 \cdot x \equiv 24 \pmod{30}$.

5.36 Mehrdeutige Division im Restklassenring

Der Lösbarkeitssatz 5.28 sagt uns, dass die Gleichung wegen $\text{ggT}(64, 84) = 4$ genau vier paarweise nicht-84-kongruente Lösungen besitzt, und zwar

$$x_0 + i \cdot \frac{84}{4}, \text{ also } x_0 + i \cdot 21 \quad (\circ) \quad \text{mit } i = 0, 1, 2, \text{ bzw. } 3,$$

wobei x_0 die (mod 21) einzige Lösung von

$$\frac{64}{4} \cdot x \equiv \frac{16}{4} \pmod{21}, \text{ also } 16 \cdot x \equiv 4 \pmod{21}, \text{ also auch } (\#) \quad 4 \cdot x \equiv 1 \pmod{21}$$

ist. Die Kongruenz- bzw. Restklassenrechenregeln führen von (#) zu

$$\begin{aligned} 4 \cdot x &\equiv -20 \pmod{21} \\ x &\equiv -5 \pmod{21} \\ x &\equiv 16 \pmod{21} \end{aligned}$$

(\circ) liefert dann die Lösungen 16, 37, 58 und 79 (jeweils mod 84).

5.37 Zahlen mit vorgegebenen Divisionsresten

- a) Wir gehen wie im Beweis des Chinesischen Restwertesatzes vor und setzen bzw. erhalten der Reihe nach:

$$k = 3, m_1 = 3, m_2 = 5, m_3 = 7, r_1 = 2, r_2 = 3, r_3 = 2$$

$$m = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 5 \cdot 7 = 105$$

$$M_1 = 5 \cdot 7 = 35, M_2 = 3 \cdot 7 = 21, M_3 = 3 \cdot 5 = 15$$

Wir gewinnen aus der Berechnung des ggT 1 der Paare M_i, m_i ganzzahlige Koeffizienten s_i, t_i für $s_i \cdot M_i + t_i \cdot m_i = 1$ – wie im Beweis des Lemmas von Bézout:

- $s_1 \cdot 35 + t_1 \cdot 3 = 1$:
 $35 = 11 \cdot 3 + 2$ & $3 = 1 \cdot 2 + 1 \Rightarrow 1 = 3 - 2 = 3 - (35 - 11 \cdot 3) = -1 \cdot 35 + 12 \cdot 3$
- $s_2 \cdot 21 + t_2 \cdot 5 = 1$:
 $21 = 4 \cdot 5 + 1 \Rightarrow 1 = 1 \cdot 21 - 4 \cdot 5$
- $s_3 \cdot 15 + t_3 \cdot 7 = 1$:
 $15 = 2 \cdot 7 + 1 \Rightarrow 1 = 1 \cdot 15 - 2 \cdot 7$

Die Koeffizienten $s_1 = -1, s_2 = s_3 = 1$ gehen ein in ein passendes x :

$$\begin{aligned} x &= s_1 \cdot M_1 \cdot r_1 + s_2 \cdot M_2 \cdot r_2 + s_3 \cdot M_3 \cdot r_3 \\ &= (-1) \cdot 35 \cdot 2 + 1 \cdot 21 \cdot 3 + 1 \cdot 15 \cdot 2 \\ &= 23 \end{aligned}$$

Alle Lösungen gleichen einander mod m , und $m = 105$; insofern ist 23 die kleinste und 128 die nächstgrößere.

- b) Spielen wir den Chinesischen Restwertsatz nun mit

$$k = 4, m_1 = 3, m_2 = 4, m_3 = 5, m_4 = 7, r_1 = 1, r_2 = 1, r_3 = 1, r_4 = 0$$

$$m = m_1 \cdot m_2 \cdot m_3 \cdot m_4 = 3 \cdot 4 \cdot 5 \cdot 7 = 420$$

$$M_1 = 140, M_2 = 105, M_3 = 84, M_4 = 60$$

durch, geht es weiter mit

- $s_1 \cdot 140 + t_1 \cdot 3 = 1$:
 $140 = 46 \cdot 3 + 2$ & $3 = 1 \cdot 2 + 1 \Rightarrow 1 = 3 - 2 = 3 - (140 - 46 \cdot 3) = -1 \cdot 140 + 47 \cdot 3$
 - $s_2 \cdot 105 + t_2 \cdot 4 = 1$:
 $105 = 26 \cdot 4 + 1 \Rightarrow 1 = 105 - 26 \cdot 4$
 - $s_3 \cdot 84 + t_3 \cdot 5 = 1$:
 $84 = 16 \cdot 5 + 4$ & $5 = 1 \cdot 4 + 1 \Rightarrow 1 = 5 - 4 = 5 - (84 - 16 \cdot 5) = -1 \cdot 84 + 17 \cdot 5$
 - $s_4 \cdot 60 + t_4 \cdot 7 = 1$:
 $60 = 8 \cdot 7 + 4$ & $7 = 1 \cdot 4 + 3$ & $4 = 1 \cdot 3 + 1$
 $\Rightarrow 1 = 4 - 3 = 4 - (7 - 4) = 2 \cdot (60 - 8 \cdot 7) - 7 = 2 \cdot 60 - 17 \cdot 7$
- $$\begin{aligned} x &= s_1 \cdot M_1 \cdot r_1 + s_2 \cdot M_2 \cdot r_2 + s_3 \cdot M_3 \cdot r_3 + s_4 \cdot M_4 \cdot r_4 \\ &= (-1) \cdot 140 \cdot 1 + 1 \cdot 105 \cdot 1 + (-1) \cdot 84 \cdot 1 + 2 \cdot 60 \cdot 0 \\ &= -119 \end{aligned}$$

Weitere x unterscheiden sich um Vielfache von 420. Das kleinste Positive x ist also 301.

[Es geht aber auch ohne derart „schweres Gerät“. Die Lösung minus 1 muss ein Vielfaches von 60 sein (warum?). Also suchen wir unter den Zahlen 1, 61, 121 usw. nach Vielfachen von 7 und werden bei 301 fündig (Warum sind nicht alle keine Vielfachen von 7?).]

5.38 Ein Skatblatt als Restklassenring \mathbb{Z}_{32}

- a) 0001110100, 0101110001 usw.

[Man kann sich auch jeweils auf die ersten 8 Folgenglieder beschränken und die Folgen zyklisch lesen. Dies sind dann sogenannte De-Bruijn-Folgen – hier für die Alphabetgröße $k = 2$ und die Teilwortlänge $n = 3$ – die per Definition der Länge k^n sind und zyklisch gelesen alle Wörter der Länge 5 als Teilwörter enthalten.]

- b) Das 5-fache Abheben ist Bluff; es soll nur gutes Mischen vortäuschen. In Wahrheit werden die Karten beim Abheben lediglich um $k_1 + k_2 + k_3 + k_4 + k_5$ Positionen zyklisch verschoben, behalten also (wie die Restklassen 1 bis 32 in \mathbb{Z}_{32}) ihre zyklische Reihenfolge. Die Karten sind anfangs bezüglich „rot“ (1) und „schwarz“ (0) so anzuordnen, dass die Fünferblöcke (Karte Nr. $i, i+1, i+2, i+3, i+4$, zyklisch gezählt) für jedes i zwischen 1 und 32 eine andere Farbenfolge, z.B. 01101, haben. Und daran ändert das Abheben ja nichts.

Der Zauberer merkt sich die Reihenfolge der 32 Karten (was für manche an echte Zauberei grenzen mag) und kann an der Rot-Schwarz-Information für die Karten Nr. $i, i+1, i+2, i+3, i+4$ (gerechnet in \mathbb{Z}_{32}) das i ablesen und somit die Karten aufzählen.

Es erhebt sich die Frage, ob es eine solche Anordnung, eine De-Bruijn-Folge (s.o.) für 2 und 5, gibt. Die Antwort ist ja, sogar viele. Intelligentes Raten oder systematisches Durchprobieren ergibt mit Zeit und Geduld eine Lösung wie

00000100011001010011101011011111.

[In [Bogo 2014]¹ wird gezeigt, wie man eine De-Bruijn-Folge für Wörter der Länge n über dem Alphabet $A = \{0, \dots, k-1\}$ rascher findet:

- Schreibe eine Folge von n Zahlen aus A .
- Hänge so lange wie möglich an die bisherige Folge die größtmögliche der Zahlen 0 bis $k-1$ so an, dass die letzten n Zahlen ein neues n -Teilwort bilden.
- (Wenn also mit keiner der k Zahlen ein neues n -Teilwort entstehen kann ...) Streiche die letzten $n-1$ Ziffern.]

5.39 Addition und Ordnungsrelation

- Aus der induktiven Definition von $<$ folgt:
Wenn man an die Strichliste m einen Strich anhängt, ist die erhaltene Strichliste größer als m : $m < m|$ (strenger ausgedrückt: ist m kleiner als die erhaltene Strichliste). Und daher ist auch die Strichliste nach Anhängen eines weiteren Striches größer als m : $m < m||$, usw. So erhält man der Reihe nach jede größere Strichliste: $m < n \Rightarrow n$ ist $m|$, $m||$ oder ein $m|\dots|$.
Nennen wir nun im Falle $m < n$ die hinter m angehängte Strichliste d , so ist n die Strichliste, die entsteht, wenn wir d an m anhängen.
- Aus der induktiven Definition von $+$ folgt:
Aus m entsteht $m + d$ auf folgende Weise: Man baut „gleichzeitig“ d strichweise auf, und für jeden Strich, den man dabei bis zum fertigen d schreibt, hängt man auch an m , bzw. das mittlerweile verlängerte m , einen Strich an.
Wenn d fertig ist, haben wir gleichzeitig die Strichliste von d an m angehängt und so $m + d$ erhalten.
- Insgesamt sind also die Strichlisten von n und $m + d$ identisch.

¹ [Bogo 2014] A. Bogomolny, Constructive Existence of the de Bruijn Cycles, Interactive Mathematics Miscellany and Puzzles, <http://www.cut-the-knot.org/arithmetic/combinatorics/deBruijnCyclesAlgorithm.shtml>, Gelesen 28. November 2014