B Lösungen der Aufgaben

Zu Kapitel 1

1.1. Es kommt gar nicht darauf an, dass p eine Primzahl ist. Wir benutzen nur, dass p keine Potenz von 10 ist, denn aus $\log_{10}(p) = r/s$ folgt $\log_{10}(p^s) = r$ und damit $p^s = 10^r$.

1.2. (a) Euklidischer Algorithmus:

$$\begin{aligned} 56 &= 2 \cdot 35 - 14, && \text{d. h. } 14 = 2 \cdot 35 - 56 \\ 35 &= 2 \cdot 14 + 7, && \text{d. h. } \quad 7 = 35 - 2 \cdot 14 \\ 14 &= 2 \cdot 7, && \text{d. h. } \quad 7 = \mathrm{ggT}(35, 56) \end{aligned}$$

Einsetzen der ersten Gleichung in die zweite liefert $7 = 35 - 2 \cdot (2 \cdot 35 - 56) = -3 \cdot 35 - (-2) \cdot 56$, d. h. $x = -3,\ y = -2$.

1.2. (b)

$$\begin{aligned} 7 &= -3 \cdot 35 + \frac{56}{7} \cdot 35 - \frac{35}{7} \cdot 56 + 2 \cdot 56 \\ &= \left(\frac{56}{7} - 3\right) \cdot 35 - \left(\frac{35}{7} - 2\right) \cdot 56 \\ &= 5 \cdot 35 - 3 \cdot 56, \ \text{d. h. } x = 5,\ y = 3 \end{aligned}$$

1.3. Die Lösungen der beiden separaten Kongruenzen $3x \equiv 0 \mod 13$ und $-7y \equiv 11 \mod 13$ ergeben durch Addition auf alle Fälle Lösungen der Kongruenz $3x - 7y \equiv 11 \mod 13$. Sei $x_0 = 0$ eine spezielle Lösung von $3x \equiv 0 \mod 13$ und $y_0 = 4$ eine spezielle Lösung von $-7y \equiv 11 \mod 13$. Damit erhalten wir in $3x_0 - 7y_0$ eine zur Aufspaltung $11 = 0 + 11$ gehörige spezielle Lösung der ursprünglichen Kongruenz. Die zu x_0, y_0 gehörige allgemeine Lösung der ursprünglichen Kongruenz hat dann die Gestalt

$$3x_0 - 7y_0 + 13t = 3(x_0 + u) - 7(y_0 + v)$$

wobei $3u \equiv 7v \mod 13$ gelten muss. Für $u = 1$ ergibt sich $3 \equiv 7 \cdot 6 \mod 13$, also $3s \equiv 7 \cdot 6 \cdot s \mod 13$ mit beliebigem $s \in \mathbb{Z}$. Für die allgemeine Lösung erhalten wir also $x = s, y = 4 + 6s$, also $3s - 7(4 + 6s) \equiv 11 \mod 13$ für alle $s \in \mathbb{Z}$.

1.4. Jeder gemeinsame Teiler von $a + b$ und $a - b$ teilt auch $2a$ und $2b$. Die Behauptung folgt nun aus $\mathrm{ggT}(2a, 2b) = 2$.

1.5. (a) Sei $n = \sum_{k=0}^{\ell} a_k 10^k$. Dann ist die Quersumme $q(n) = \sum_{k=0}^{\ell} a_k$. Wegen $10 \equiv 1 \bmod 3$ folgt $n \equiv q(n) \bmod 3$. Dies beweist die *Dreierregel zur Division*.

1.5. (b) Sei wieder $n = \sum_{k=0}^{\ell} a_k 10^k$. Dann ist $10^k \equiv (-1)^k \bmod 11$. Es folgt die *Elferregel zur Division*: $n \equiv \sum_{k=0}^{\ell} (-1)^k a_k \bmod 11$. Ein Zahl ist also genau dann durch 11 teilbar, wenn ihre alternierende Quersumme durch 11 teilbar ist.

1.6. $\Rightarrow$: Sei n zusammengesetzt, $n = pq$ mit $1 < p, q < n$. Dann ist p Teiler von $(n-1)!$, aber nicht von -1, da p kein Inverses in $(\mathbb{Z}/n\mathbb{Z})^*$ besitzt.
$\Leftarrow$: $(n-1)!$ ist das Produkt der Zahlen in $M = \{2, \ldots, n-1\}$. Ist n prim, so sind alle Elemente in M modulo n invertierbar und nur für $x \in M$ mit $x = n-1$ gilt $x \equiv x^{-1} \bmod n$. Fasse die Elemente aus $M \setminus \{n-1\}$ durch Umordnung paarweise mit ihren Inversen modulo n zusammen. Das Produkt über diese Zahlen ist damit 1 modulo n. Daher ist $(n-1)! \equiv n-1 \equiv -1 \mod n$.

1.7. $n^4 + 4^n$ ist niemals 2, also können wir annehmen, dass $n = 2k+1$ ungerade ist mit $k \geq 1$. Setze $x = n$ und $y = 2^k$, dann ist $n^4 + 4^n = x^4 + 4y^4$, denn $4y^4 = 4 \cdot 2^{4k} = 4^{2k+1}$. Schließlich ergibt sich: $x^4 + 4y^4 = (x^2 + 2y^2)^2 - 4x^2y^2 = (x^2 + 2y^2 + 2xy)(x^2 + 2y^2 - 2xy)$. Sind jetzt $x, y \in \mathbb{N}$ mit $y > 1$, so gilt $x^2 + 2y^2 + 2xy \geq x^2 + 2y^2 - 2xy \geq (x-y)^2 + y^2 \geq 4$. Insbesondere ist ist $x^4 + 4y^4$ keine Primzahl.

1.8. (a) Angenommen $n = pq$ mit $p, q > 1$. Betrachte die Identität

$$x^q - y^q = (x-y) \sum_{i=0}^{q-1} x^i y^{q-1-i} \tag{B.1}$$

mit $x = 2^p$ und $y = 1$. Primzahlen der Form $2^n - 1$ bezeichnet man als Mersenne-Primzahlen (nach Marin Mersenne, 1588–1648).

1.8. (b) Angenommen $n = r2^m$ mit $r > 1$ ungerade. Dann gilt $2^{r2^m} + 1 = (2^{2^m})^r - (-1)^r$. Aus Gleichung (B.1) mit $x = 2^{2^m}$, $y = -1$ und $q = r$ ergibt sich wieder eine nichttriviale Faktorisierung. Primzahlen der Form $2^n + 1$ bezeichnet man als Fermat-Primzahlen.

1.8. (c) Sei ohne Einschränkung $1 \leq m < n$. Sei $d \in \mathbb{N}_1$ mit $d \mid f_m$ und $d \mid f_n$. Es gilt

$$\frac{f_n - 2}{f_m} = \frac{2^{2^n} - 1}{2^{2^m} + 1} = (2^{2^m})^{2^{n-m}-1} - (2^{2^m})^{2^{n-m}-2} + \cdots - 1$$

Damit ist $f_m \mid (f_n - 2)$ und folglich $d \mid (f_n - 2)$. Wegen $d \mid f_n$ folgt also $d \mid 2$. Aber es ist $d \neq 2$, da f_n und f_m beide ungerade sind. Da die Zahlen f_n paarweise teilerfremd sind und jedes f_n mindestens einen Primteiler hat, muss die Folge der Primzahlen unendlich sein.

1.9. Die Lösung lautet 111: Die beiden Forderungen $x \equiv 1 \bmod 2$ und $x \equiv 0 \bmod 3$ sind äquivalent mit $x \equiv 3 \bmod 6$. Nehmen wir die dritte Gleichung hinzu, so muss $3 + 6k \equiv 1 \bmod 5$ gelten. Daraus folgt $k \equiv 3 \bmod 5$ sowie $x \in 21 + 30\ell$ für ein $\ell \in \mathbb{N}$. Die letzte Gleichung verlangt $21 + 30\ell \equiv 6 \bmod 7$, also $2\ell \equiv 6 \bmod 7$. Dies ist äqivalent mit $\ell \equiv 3 \bmod 7$. Wir erhalten die eindeutige Lösung $x = 21 + 30 \cdot 3 = 111$. Sie ist die einzige positive Lösung im Bereich bis $\mathrm{kgV}\{2, 3, 5, 7\} = 210$.

1.10. Sei x_0 eine Lösung des gegebenen Systems. Dann gilt $x_0 - a = rn$ und $x_0 - b = sm$ und folglich $a - b = (x_0 - b) - (x_0 - a) = sm - rn$. Wir setzen $d = \mathrm{ggT}(n, m)$.

Die Linearkombination $sm - rn$ ist ein Vielfaches von d. Also gilt $d \mid (a - b)$. Sei umgekehrt $d \mid (a - b)$. Dann gilt $a - b = kd$. Ferner gibt es eine Darstellung $d = nx + my$. Folglich ist $a - knx = b + kmy = x_0$ eine Lösung des Systems. Sei $t = \mathrm{kgV}(n, m)$. Dann gilt $dt = nm$. Ferner gibt es $v, w \in \mathbb{Z}$ mit $n = vd$, $m = wd$. Folglich ist $t = vwd$. Sei nun x_0 eine Lösung des gegebenen Systems. Dann gilt $x_0 \equiv a \mod vd$ und $x_0 \equiv b \mod wd$. Wegen $t = vwd$ sind damit die Kongruenzen $x_0 + kt \equiv a \mod vd$ und $x_0 + kt \equiv b \mod wd$ für beliebige $k \in \mathbb{Z}$ erfüllt; d. h., x_0 ist eindeutig modulo $t = \mathrm{kgV}(n, m)$.

1.11. (a) Nach dem kleinen Satz von Fermat gilt $n^5 \equiv n \mod 2$, $n^5 \equiv n \mod 3$ und $n^5 \equiv n \mod 5$. Mit dem Chinesischen Restsatz folgt $n^5 \equiv n \mod 30$.

1.11. (b) Es gilt

$$3^{n^4+n^2+2n+4} \equiv 0 \equiv 21 \mod 3 \tag{B.2}$$

$$3^{n^4+n^2+2n+4} \equiv 1 \equiv 21 \mod 4 \tag{B.3}$$

$$3^{n^4+n^2+2n+4} \equiv 1 \equiv 21 \mod 5 \tag{B.4}$$

Hierbei gilt (B.2), da die linke Seite für alle $n \in \mathbb{N}$ durch 3 teilbar ist. Die Gleichung (B.3) ist wahr, da für die Basis $3 \equiv -1 \mod 4$ gilt und der Exponent für alle $n \in \mathbb{N}$ gerade ist. Da $\mathrm{ggT}(3, 5) = 1$ gilt, folgt (B.4) aus dem kleinen Satz von Fermat, denn für den Exponenten gilt $n^4 + n^2 + 2n + 4 \equiv 0 \mod 4$. Diese Kongruenz rechnet man leicht für alle $n \in \{-1, 0, 1, 2\}$ nach. Die Behauptung folgt nun aus dem Chinesischen Restsatz.

1.11. (c) Mit $64 \equiv 7 \mod 57$ ergibt sich $7^{n+2} + 8^{2n+1} = 49 \cdot 7^n + 8 \cdot (8^2)^n = 49 \cdot 7^n + 8 \cdot (64)^n \equiv 49 \cdot 7^n + 8 \cdot 7^n = 57 \cdot 7^n \equiv 0 \mod 57$.

1.12. Aus $\mathrm{ggT}(a, p) = 1$ folgt mit dem kleinen Satz von Fermat, dass $a^{p-1} \equiv 1 \mod p$. Da $p - 1 = 2k$ gerade ist, folgt aus $\mathrm{ggT}(a, 4) = 1$ mit dem Satz von Euler $a^{p-1} = a^{2k} = (a^{\varphi(4)})^k \equiv 1^k \equiv 1 \mod 4$. Wegen $\mathrm{ggT}(4, p) = 1$ ergibt sich die Behauptung nun mit dem Chinesischen Restsatz.

1.13. (a) $|(\mathbb{Z}/51\mathbb{Z})^*| = \varphi(51) = \varphi(3)\varphi(17) = 2 \cdot 16 = 32$.

1.13. (b) Es gilt $\varphi(51) = 32 = 3 \cdot 11 - 1$. Damit gilt $3 \cdot 11 \equiv 1 \mod 32$ und es ergibt sich der geheime Schlüssel $s = 3$.

1.13. (c) $7^3 \equiv 49 \cdot 7 \equiv -2 \cdot 7 \equiv -14 \equiv 37 \mod 51$, d. h. $x = 37$.

1.13. (d) Nach dem Satz von Lagrange 1.22 teilt die Ordnung eines Elements die Gruppenordnung; da 10 kein Teiler von 32 ist, gibt es keine Elemente der Ordnung 10.

1.13. (e) Sowohl in $(\mathbb{Z}/3\mathbb{Z})^*$ als auch in $(\mathbb{Z}/17\mathbb{Z})^*$ haben alle Elemente a die Eigenschaft $a^{16} = 1$. Nach dem Chinesischen Restsatz haben auch in $(\mathbb{Z}/51\mathbb{Z})^*$ alle Elemente diese Eigenschaft. Insbesondere gibt es keine Elemente der Ordnung 32. Also ist $(\mathbb{Z}/51\mathbb{Z})^*$ nicht zyklisch.

1.14. Wider Erwarten hat der Haushaltsausschuss diesmal richtig gelegen. Es kommt nach dem chinesischen Restsatz und bis auf Symmetrie in p und q nur darauf an, dass immer $x^{es} \equiv x \mod p$ gilt. Dies ist schon erfüllt, wenn $es \equiv 1 \mod k$ für ein Vielfaches $k \in (p-1)\mathbb{Z}$ gilt. Nach Auflösung der Symmetrie reicht uns $k \in \mathrm{kgV}(p-1, q-1)\mathbb{Z}$. Für $p = 7$ und $q = 19$ mit $e = 5$ hätte der Haushaltsausschuss $s = 11$ statt $s = 65$ empfohlen.

1.15. (a) Es gilt $d(c(x)) = (x^e \bmod n)^s \bmod n \equiv x^{es} \equiv x^{1+k(p-1)} \equiv x \bmod p$ für $k \in \mathbb{N}$. Analog zeigt man $d(c(x)) \equiv x \bmod q$ und $d(c(x)) \equiv x \bmod r$. Mit dem Chinesischen Restsatz folgt $d(c(x)) \equiv x \bmod n$. Mit $x \in \{0, \ldots, n-1\}$ erhalten wir schließlich $d(c(x)) = x$.

1.15. (b) Es gilt $\varphi(66) = 20$ und $1 \equiv 21 = 3 \cdot 7 \equiv 3 \cdot 27 \bmod 20$. Dies liefert den Enschlüsselungsexponenten $s = 3$. Es folgt $14^3 \equiv 0^3 \equiv 0 \mod 2$, $14^3 \equiv (-1)^3 \equiv -1 \equiv 2 \mod 3$ und $14^3 \equiv 3^3 \equiv 27 \equiv 5 \mod 11$. Mit dem chinesischen Restsatz erhalten wir $x = 38$.

1.16. Da Oskar die teilerfremden Zahlen e_1 und e_2 kennt, kann er mit Hilfe des euklidischen Algorithmus Zahlen $a, b \in \mathbb{Z}$ mit $ae_1 + be_2 = 1$ berechnen. Mit ihnen und den verschlüsselten Nachrichten $m^{e_1} \bmod n$ und $m^{e_2} \bmod n$ erhält er $(m^{e_1})^a \cdot (m^{e_2})^b = m^{ae_1+be_2} \equiv m \bmod n$.

1.17. Wenn zwei der Zahlen n_1, n_2, n_3 nicht teilerfremd sind, kann Oskar deren größten gemeinsamen Teiler berechnen und erhält damit eine Faktorisierung. Nehmen wir also an, dass n_1, n_2 und n_3 teilerfremd sind. Dann kann aus den verschlüsselten Nachrichten $m^3 \bmod n_i$ mit Hilfe des chinesischen Restsatzes eine Zahl $x \in \{1, \ldots, n_1 \cdot n_2 \cdot n_3\}$ mit $x \equiv m^3 \bmod n_1 \cdot n_2 \cdot n_3$ bestimmt werden. Da $m < n_i$ ist, folgt $m^3 < n_1 \cdot n_2 \cdot n_3$ und somit $x = m^3$. Also kann die Nachricht $m = \sqrt[3]{x}$ durch Wurzelziehen bestimmt werden.

1.18. Aus Satz 1.19 folgt $a^{\varphi(b)} + b^{\varphi(a)} \equiv a^{\varphi(b)} \equiv 1 \bmod b$. Analog gilt $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \bmod a$. Da a und b teilerfremd sind, impliziert der chinesische Restsatz $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \bmod ab$.

1.19. (a) Es ist $F_1 = F_3 - F_2, \ldots, F_{n-1} = F_{n+1} - F_n$. Aufsummieren ergibt $F_1 + \cdots + F_n = F_{n+2} - F_2 = F_{n+2} - 1$.

1.19. (b) Für $n = 0$ gilt $\sum_{k=0}^{0} F_k^2 = F_0^2 = 0 \cdot 0 = 0 = 0 \cdot 1 = F_0 F_1$. Für $n > 0$ ergibt sich $\sum_{k=0}^{n} F_k^2 = \sum_{k=0}^{n-1} F_k^2 + F_n^2 = F_{n-1}F_n + F_n^2 = F_n(F_{n-1} + F_n) = F_n F_{n+1}$.

1.19. (c) Für $k = 1$ ist dies trivial. Sei daher $k > 1$. Dann gilt:

$$\begin{aligned} F_k F_{n+1} + F_{k-1} F_n &= (F_{k-1} + F_{k-2}) F_{n+1} + F_{k-1} F_n \\ &= F_{k-1} F_{n+1} + F_{k-2} F_{n+1} + F_{k-1} F_n \\ &= F_{k-1}(F_{n+1} + F_n) + F_{k-2} F_{n+1} \\ &= F_{k-1} F_{n+2} + F_{k-2} F_{n+1} \\ &= F_{(n+1)+(k-1)} = F_{n+k} \end{aligned}$$

1.19. (d) 1. *Mit Induktion*: Es ist $F_2F_0 - F_1^2 = -1$ und für $n > 1$ gilt:

$$\begin{aligned} F_{n+1}F_{n-1} - F_n^2 &= (F_n + F_{n-1})F_{n-1} - F_n^2 \\ &= F_nF_{n-1} + F_{n-1}^2 - F_n^2 \\ &= F_n(F_{n-1} - F_n) + F_{n-1}^2 \\ &= -F_nF_{n-2} + F_{n-1}^2 \\ &\overset{\text{IV}}{=} -(-1)^{n-1} = (-1)^n \end{aligned}$$

2. *Matrixbeweis*: Nach Gleichung (1.4) gilt $\left(\begin{smallmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)^n$. Die Determinante von $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ ist -1, also ist die Determinante der rechten Seite gerade $(-1)^n$. Die Determinante der linken Matrix ist $F_{n+1}F_{n-1} - F_n^2$. Dies zeigt die Behauptung.

1.20. (a) Da f^p die identische Abbildung ist, ist f eine Bijektion. Angenommen $f^i(m) = f^j(m)$ für ein $1 \le i < j \le p$. Dann gilt $f^q(m) = m$ für $q = j - i < p$. Es folgt $f^{\mathrm{ggT}(p,q)}(m) = m$ und dann $f(m) = m$, denn $\mathrm{ggT}(p,q) = 1$. Wegen $f(m) = m$ ist $f^k(m) = m$ für alle $k \in \mathbb{N}$.

1.20. (b) Die Relation $m \sim n$, falls $f^i(m) = f^j(n)$ für gewisse $i, j \in \mathbb{N}$, ist eine Äquivalenzrelation. Nach Aufgabe 1.20. (a) hat die Klasse von einem $m \in M \setminus F$ genau p Elemente. Die Anzahl der Nicht-Fixpunkte ist also durch p teilbar.

1.21. (a) Wir führen den Beweis induktiv nach n: Für $n \in \{1, 2\}$ ist die Gleichung jeweils erfüllt. Weiterhin gilt:

$$\begin{aligned} L_{n+2} = L_{n+1} + L_n &\overset{\text{IV}}{=} (F_{n+2} + F_n) + (F_{n+1} + F_{n-1}) \\ &= (F_{n+2} + F_{n+1}) + (F_n + F_{n-1}) = F_{n+3} + F_{n+1} \end{aligned}$$

1.21. (b) Es gilt $\mathcal{L}_1 = \{\emptyset\}$, denn 1 folgt nach 1 modulo 1. Die Menge $\mathcal{L}_2$ besteht aus den drei Teilmengen $\emptyset$, $\{1\}$ und $\{2\}$. Sei also $n \ge 3$. Rechnen wir nicht modulo n, so ist die Anzahl der entsprechenden Teilmengen von $\{1, \ldots, n\}$ gerade die Anzahl Wörter über den Buchstaben a, b, in denen keine zwei a's hintereinander stehen. Nach Beispiel 1.25 gibt es hiervon F_{n+2} Wörter. Angenommen, wir rechnen jetzt modulo n. Die Anzahl der Teilmengen $M \in \mathcal{L}_n$ mit $1 \notin M$ ist daher F_{n+1}, denn die Einschränkung, dass 1 der Nachfolger von n ist, kommt nicht zur Geltung. Betrachte jetzt die Teilmengen $M \in \mathcal{L}_n$ mit $1 \in M$. Dann können die Positionen 2 und n nicht besetzt werden. Ferner ist $2 < n$. Also ist die Anzahl solcher M (erneut nach Beispiel 1.25) gerade F_{n-1}. Die Behauptung folgt aus Aufgabe 1.21. (a).

1.21. (c) Sei $f : \mathcal{L}_p \to \mathcal{L}_p$ definiert durch $f(M) = \{i + 1 \bmod n \mid i \in M\}$. Dann gilt $f^p(M) = M$ für alle $M \in \mathcal{L}_p$. Der einzige Fixpunkt von f ist $M = \emptyset$. Nach Aufgabe 1.20. ist daher $|\mathcal{L}_p| \equiv 1 \bmod p$.

1.22. $F_0 = 0$ und $F_1 = 1$ zusammen mit Gleichung (1.2) definiert die Zahlen $F_n \in \mathbb{F}$ für alle $n \in \mathbb{Z}$. Wähle $q \in K$ mit $q^2 = 5$. Dann ist q eine Lösung der quadratischen

Gleichung $x^2 - 5$; und es gilt $x^2 - 5 = (x - q)(x + q)$ für alle $x \in \mathbb{F}$. Daher ist q bis auf das Vorzeichen eindeutig definiert. Wir schreiben $q = \sqrt{5}$ und setzen $\varphi = \frac{1+\sqrt{5}}{2}$ sowie $\hat{\varphi} = \frac{1-\sqrt{5}}{2}$. Dies ist möglich, denn 2 ist invertierbar. Ferner gilt $\varphi - \hat{\varphi} \neq 0$, da 5 invertierbar ist. Der Beweis von Gleichung (1.3) aus Abschnitt 1.11 kann nun wörtlich übernommen werden.

In $\mathbb{Z}/11\mathbb{Z}$ gilt $F_{10} = 0$ nach Gleichung (1.3) und dem kleinen Satz von Fermat. Außerdem gilt $4^2 = 16 \equiv 5 \bmod 11$ sowie $2^{-1} \equiv 6 \bmod 11$. Mit $\varphi = -3$ und $\hat{\varphi} = 4$ ist der goldenen Schnitt -3 oder 4. Nach dem kleinen Satz von Fermat gilt nun $F_{12} = \frac{\varphi^2 - \hat{\varphi}^2}{\varphi - \hat{\varphi}} = \varphi + \hat{\varphi} = 1$.

1.23. (a) Zunächst sei $\sqrt{5}$ ein neues Symbol. Wir setzen $\mathbb{F} = \mathbb{F}_p \times \mathbb{F}_p$ und schreiben ein Paar $(a, b) \in \mathbb{F}$ als Summe $a + b\sqrt{5}$. Wir addieren komponentenweise und multiplizieren durch $(a + b\sqrt{5})(c + d\sqrt{5}) = ac + 5bd + (ad + bc)\sqrt{5}$. Assoziativ- und Distributivgesetze können direkt verifiziert werden. Wir können $\mathbb{Z}/p\mathbb{Z}$ in $\mathbb{F}$ vermöge $a \mapsto a + 0\sqrt{5}$ einbetten und sehen auch, dass $\sqrt{5}^2 = (0 + \sqrt{5})^2 = 5 + 0\sqrt{5} = 5$ gilt. In $\mathbb{F}$ ist 5 also ein Quadrat. Hierfür wird weder benötigt, dass p eine Primzahl ist noch dass 5 kein Quadrat in $\mathbb{Z}/p\mathbb{Z}$ ist. Wir benötigen diese Eigenschaften, um zu zeigen, dass $\mathbb{F}$ ein Körper ist. Zunächst sind alle Elemente $(a, 0)$ und $(0, a)$ invertierbar, sofern $a \neq 0$ gilt, da p eine Primzahl ungleich 5 ist. Es reicht daher, ein Inverses zu $1 + b\sqrt{5}$ zu finden. Nach der binomischen Formel gilt $(1 + b\sqrt{5})(1 - b\sqrt{5}) = 1 - 5b^2$. Da 5 kein Quadrat ist, ist dies ein von Null verschiedenes Element $c \in \mathbb{F}_p$. Das Inverse zu $1 + b\sqrt{5}$ erhalten wir nun durch $(1 - b\sqrt{5})c^{-1}$.

1.23. (b) Es gilt $\sqrt{5}^{2p} = 5^p = 5 \in \mathbb{F}$ nach dem kleinen Satz von Fermat. Also ist $\sqrt{5}^p \in \mathbb{F}$ ein Element, dessen Quadrat 5 ist. Hieraus folgt $\sqrt{5}^p = \pm\sqrt{5}$, denn $q^2 = 5$ ist in $\mathbb{F}$ äquivalent mit $(q - \sqrt{5})(q + \sqrt{5}) = 0$. Der Binomialsatz $(1 + y)^p = \sum_{k=0}^{p} \binom{p}{k} y^{p-k}$ kann sehr leicht mit Induktion im Vorgriff auf Satz 4.3 bewiesen werden. Alle Binomialkoeffienten $\binom{p}{k}$ sind für $1 \leq k < p$ kongruent 0 modulo p, denn die Primzahl p kann bei $\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots(p-k+1)}{k!}$ nicht gekürzt werden. Wir erhalten $(1 + \sqrt{5})^p = 1 + \sqrt{5}^p$ und $(1 - \sqrt{5})^p = 1 - \sqrt{5}^p$. Hieraus folgt die Behauptung, da nach dem kleinen Fermat $2^p = 2$ gilt.

1.24. Für $p = 2$ und $p = 5$ überprüfen wir die Behauptung direkt. Sei also $2 \neq p \neq 5$. Mit $\mathbb{F}_p$ bezeichnen wir den Körper $\mathbb{Z}/p\mathbb{Z}$ und setzen $\mathbb{F} = \mathbb{F}_p$, falls 5 ein Quadrat ist in $\mathbb{F}_p$. Ansonsten adjungieren wir $\sqrt{5}$ und betrachten $\mathbb{F} = \mathbb{F}_p(\sqrt{5})$ entsprechend Aufgabe 1.23.. Wir verwenden mehrfach den kleinen Satz von Fermat und setzen $\varphi = \frac{1+\sqrt{5}}{2}$.

1. *Herleitung*: Nach Aufgabe 1.22. können wir Gleichung (1.3) benutzen, und Aufgabe 1.23. (b) zeigt $\{\varphi^p, \hat{\varphi}^p\} = \{\varphi, \hat{\varphi}\}$. Wir unterscheiden zwei Fälle. Im ersten Fall gelte $\varphi^p = \varphi$, also auch $\hat{\varphi}^p = \hat{\varphi}$. (Dies ist insbesondere der Fall, wenn 5 ein Quadrat in $\mathbb{F}_p$ ist.) Es folgt $\varphi^{p-1} = \hat{\varphi}^{p-1} = 1$, also $F_{p-1} = 0$ und $F_p = 1$. Damit ist dann auch $F_{p+1} = 1$.

Im zweiten Fall gilt $\varphi^p = \hat{\varphi}$. (Insbesondere ist 5 kein Quadrat in $\mathbb{F}_p$.) Dann gilt auch $\hat{\varphi}^p = \varphi$. Es folgt $F_p = -1$. Wegen $\varphi \cdot \hat{\varphi} = -1$ ist ferner $F_{p+1} = 0$ und damit $F_{p-1} = 1$.

Sind wir also in einem Fall $F_{p-1} = 1$, wie etwa bei $p = 7$ mit $F_6 = 8$ oder $p = 13$ mit $F_{12} = 144$, so können wir schließen, dass 5 kein Quadrat in $\mathbb{F}_p$ ist. (Tatsächlich gilt $F_{p-1} \equiv 1 \bmod p$ genau dann, wenn 5 kein Quadrat in $\mathbb{F}_p$ ist; und $\sqrt{5}^p = -\sqrt{5}$ ist äquivalent mit $F_{p-1} = 1$.)

2. *Matrixbeweis*: Wir benutzen Kenntnisse der linearen Algebra. Die Spur der Matrix $\left(\begin{smallmatrix} F_{p-1} & F_p \\ F_p & F_{p+1} \end{smallmatrix}\right)$ ist die Summe der Diagonalelemente $F_{p+1}+F_{p-1}$. Nach Gleichung (1.4) reicht es, die Spur von $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)^p$ als $1 \in \mathbb{F}$ nachzuweisen. Hierfür diagonalisieren wir $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$. Die Eigenwerte dieser Matrix berechnen sich aus der Lösung des linearen Gleichungssystems $\lambda x = y$ und $\lambda y = x + y$. Die Eigenwerte sind also gerade $\varphi = \frac{1+\sqrt{5}}{2}$ und $\hat{\varphi} = \frac{1-\sqrt{5}}{2}$. Es gilt $\varphi \neq \hat{\varphi}$ und die Matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ kann über $\mathbb{F}$ durch $\left(\begin{smallmatrix} \varphi & 0 \\ 0 & \hat{\varphi} \end{smallmatrix}\right)$ diagonalisiert werden. Wir erhalten $\left(\begin{smallmatrix} \varphi & 0 \\ 0 & \hat{\varphi} \end{smallmatrix}\right)^p = \left(\begin{smallmatrix} \varphi^p & 0 \\ 0 & \hat{\varphi}^p \end{smallmatrix}\right)$. Die Exponentation mit p liefert nach Aufgabe 1.23. (b) nun $\{\varphi^p, \hat{\varphi}^p\} = \{\varphi, \hat{\varphi}\}$. Da die Spur einer Matrix nicht von der gewählten Basis abhängt, folgt die Behauptung wegen $\varphi + \hat{\varphi} = 1$.

1.25. Der euklidische Algorithmus berechnet auf eine Eingabe ℓ, k mit $\ell \geq k \geq 0$ wie üblich eine Folge $q_n, q_{n-1}, \ldots, q_1, 0$ mit $\ell = q_n$, $k = q_{n-1}$ und $q_1 = \mathrm{ggT}(\ell, k)$. Setzen wir $g_i = |q_i|$, so gelten $g_0 = 0$, $g_1 \geq 1$ und $g_{m+1} \geq g_m + 2g_{m-1}$ für $1 \leq m < n$. Die quadratische Gleichung $x^2 = 1 + 2x$ hat die Lösungen $x = \sqrt{2} \pm 1$. Wie in Abschnitt 1.12 erhalten wir hieraus $g_n \leq ((\sqrt{2}+1)^n + (1-\sqrt{2})^n)/2$. Dies liefert die Behauptung.

Zu Kapitel 2

2.1. (a) Für $n = 0$ gilt $(1+x)^0 = 1 = 1 + 0x$. Sei jetzt $n > 0$. Mit Induktion gilt
$(1+x)^n = (1+x)(1+x)^{n-1} \geq (1+x)(1+(n-1)x)$
$= 1 + nx + (n-1)x^2 \geq 1 + nx$.

2.1. (b) Aus $e^x \geq 1 + x$ folgt $x = e^{\ln x} \geq 1 + \ln x$. Wir zeigen $e^x \geq 1 + x$.

1. *Reihendarstellung*: Es ist $e^x = \sum_{n\geq 0} x^n/n!$. Zu zeigen ist $\sum_{n\geq 2} x^n/n! \geq 0$. Nun ist $x^n/n! \geq -x^{n+1}/(n+1)!$ für gerade n äquivalent mit $n + 1 \geq -x$. Insbesondere gilt die Behauptung für $-1 \leq x$, indem wir immer zwei Summanden zusammenfassen. Also ist $e^{x/m} > 0$ für alle x, wenn nur m groß genug ist. Deshalb ist $e^x = (e^{x/m})^m > 0$ für alle x. Schließlich ist $1 + x < 0$ für $x < -1$. Damit gilt die Behauptung für alle $x \in \mathbb{R}$.

2. *Kurvendiskussion*: Die Funktion $f(x) = e^x - x - 1$ hat ein Minimum bei $x = 0$ (die Ableitung $e^x - 1$ wird nur dort Null). Ferner geht $f(x)$ gegen Unendlich für $x \to \pm\infty$. Da $x = 0$ eine Nullstelle von f ist, ist dies also die einzige Nullstelle, und sonst gilt $f(x) > 0$. Damit ist die Ungleichung gezeigt.

2.1. (c) Für $-x \le n \ne 0$ stehen auf beiden Seiten nicht negative Zahlen. Die Behauptung folgt, indem wir auf beiden Seiten der Ungleichung die n-te Wurzel ziehen und danach in Aufgabe 2.1. (b) einsetzen.

2.1. (d) Wir betrachten die Funktion $f(x) = \ln(x+1) - \frac{x}{x+1}$. Diese hat eine Nullstelle bei $x = 0$. Ferner nimmt f dort auch ihr Minimum an, denn die Ableitung $f'(x) = \frac{1}{x+1} - \frac{1}{(x+1)^2} = \frac{x}{(x+1)^2}$ ist positiv für $x > 0$ und negativ für $x < 0$.

2.2. Wir können π sortieren, indem wir nacheinander Situationen mit $b_{\pi(i)} > b_{\pi(i+1)}$ betrachten und dann $b_{\pi(i)}$ und $b_{\pi(i+1)}$ vertauschen. Es reicht zu zeigen, dass $S(\pi)$ bei einer solchen Vertauschung nicht abnimmt. Dies ist eine rein lokale Situation, daher dürfen wir $n = 2$ annehmen. Sei also $a_1 \le a_2$ und $b_1 \le b_2$. Zu vergleichen sind die Summen $S = a_1b_1 + a_2b_2$ und $S' = a_1b_2 + a_2b_1$. Die Differenz $S - S'$ ist nicht negativ wegen $a_1b_1 + a_2b_2 - a_1b_2 - a_2b_1 = a_1(b_1 - b_2) + a_2(b_2 - b_1) = (a_2 - a_1)(b_2 - b_1)$.

2.3. Es gilt

$$H = \frac{n}{\sum_i a_i^{-1}} \ge \frac{n}{\sum_{i=1}^n (\min_j a_j)^{-1}} = \min_j a_j$$

und

$$Q = \sqrt{n^{-1} \textstyle\sum_{i=1}^n a_i^2} \le \sqrt{n^{-1} \textstyle\sum_{i=1}^n (\max_j a_j)^2} = \max_j a_j$$

Als Nächstes zeigen wir $G \le A$. Der Beweis ist mit Induktion. Für $n = 1$ ist die Ungleichung erfüllt. Sei nun $n > 1$. Sind alle a_i gleich, so gilt auch $G = A$. Andernfalls können wir ohne Einschränkung annehmen, dass $a_1 > A$ und $a_2 < A$. Nun setzen wir $y = a_1 + a_2 - A$. Dann ist $(n-1)A = y + a_3 + \cdots + a_n$ und somit ist A auch das arithmetische Mittel von $y, a_3, \ldots a_n$. Ferner gilt $yA - a_1a_2 = a_1A + a_2A - A^2 - a_1a_2 = (a_1 - A)(A - a_2) > 0$. Also folgt mit Induktion $A^n = A \cdot A^{n-1} \ge A \cdot y \cdot a_3 \cdots a_n \ge a_1 \cdots a_n$. Zu $H \le G$: Es gilt $H = n / \sum_{i=1}^n a_i^{-1} = \prod_{j=1}^n a_j / \left(n^{-1} \sum_{i=1}^n \prod_{j \ne i} a_j\right)$. Im Nenner steht hier also ein arithmetisches Mittel. Nach dem eben gezeigten ist dies größer oder gleich dem geometrischen Mittel:

$$H \le \frac{\prod_{j=1}^n a_j}{\sqrt[n]{\prod_{i=1}^n \prod_{j \ne i} a_j}} = \frac{\prod_{j=1}^n a_j}{\sqrt[n]{\left(\prod_{j=1}^n a_j\right)^{n-1}}} = G$$

Zu $A \le Q$: Wir verwenden wieder $G \le A$ und erhalten

$$\begin{aligned} \sum_{i=1}^n \sqrt{n}^{-1} \cdot a_i \Big/ \sqrt{\textstyle\sum_{j=1}^n a_j^2} &= \sum_{i=1}^n \sqrt{\sqrt{n}^{-2} \cdot \left(a_i / \sqrt{\textstyle\sum_{j=1}^n a_j^2}\right)^2} \\ &\le \sum_{i=1}^n \left(\frac{1}{2n} + \frac{a_i^2}{2 \sum_{j=1}^n a_j^2}\right) = 1 \end{aligned}$$

Durch Multiplikation mit $\sqrt{\sum_{i=1}^n a_i^2} / \sqrt{n}$ ergibt sich die gewünschte Ungleichung.

2.4. Sei $s > 1$. Die Funktion $x \mapsto \frac{1}{x^s}$ ist monoton fallend für $x > 0$. Damit ist $\frac{1}{i^s} \le \int_{i-1}^{i} \frac{1}{x^s}\,\mathrm{d}x$ und es gilt also $\sum_{i\ge 1} \frac{1}{i^s} \le 1 + \int_1^\infty \frac{1}{x^s}\,\mathrm{d}x < \infty$. Sei nun $s = 1$ und $k \ge 1$, d. h., wir betrachten die harmonische Reihe. Dann ist $\sum_{i=2^{k-1}+1}^{2^k} i^{-1} \ge \sum_{i=2^{k-1}+1}^{2^k} 2^{-k} = 1/2$. Für alle $n \ge 1$ ist also $\sum_{i=1}^{2^n} \frac{1}{i} > n/2$.

2.5. Wir zeigen $n \ln n - n \le n\,\overline{t}(n) \le n \ln n + n$. Jede Zahl k wird in der Summe $\sum_{i=1}^{n} t(i)$ genau bei den Zahlen $k, 2k, \ldots, \lfloor \frac{n}{k} \rfloor k$ einmal als Teiler gezählt. Daraus folgt $n\,\overline{t}(n) = \sum_{k=1}^{n} \lfloor \frac{n}{k} \rfloor$. Hierfür erhalten wir schließlich die Abschätzungen

$$\sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor \le \sum_{k=1}^{n} \frac{n}{k} \le n \sum_{k=1}^{n} \frac{1}{k} \le n\left(1 + \int_1^n \frac{1}{x}\,\mathrm{d}x\right) \le n + n \ln n$$

$$\sum_{k=1}^{n} \left\lfloor \frac{n}{k} \right\rfloor \ge \sum_{k=1}^{n} \left(\frac{n}{k} - 1\right) \ge -n + n \int_1^n \frac{1}{x}\,\mathrm{d}x \ge -n + n \ln n$$

2.6. Nach Gleichung (2.9) gilt $\pi(n) \le \frac{3n}{\log_2 n}$ für fast alle n. Damit muss sogar der mittlere Abstand zwischen Primzahlen wachsen. Eine elementare Lösung der Aufgabe kannte schon Euklid: Die $n-1$ Zahlen $n!+2, n!+3, \ldots, n!+n$ sind alle zusammengesetzt, da $n!+i$ für $1 \le i \le n$ durch i teilbar ist. Wenn p_i die größte Primzahl ist mit $p_i < n!+2$, dann folgt $p_{i+1} > n!+n$ und damit $p_{i+1} - p_i \ge n$.

2.7. (a) Aus $m/\log m \le \pi(m)$ folgt mit $m = p_n$, dass $p_n \le n \log p_n$ gilt (da $\pi(p_n) = n$). Für $p_n \le 2n \log n$ ist diese Ungleichung erfüllt.

2.7. (b) Für jede genügend große Zahl m gilt $\pi(m) \le 3m/\log m$ nach Gleichung (2.9). Mit $m = p_n$ ergibt sich $p_n \ge \frac{1}{3} n \log p_n$. Aus $p_n \ge n$ folgt daraus die Behauptung.

2.7. (c) *Elementare Lösung*: Angenommen, die Reihe konvergiert. Dann gilt $\sum_{i\ge k} \frac{1}{p_i} \le \frac{1}{2}$ für einen genügend großen Index k. Für $n \in \mathbb{N}$ sei M_n die Menge der Zahlen aus $\{1, \ldots, n\}$, deren Primteiler alle kleiner als p_k sind. Jede Zahl $x \in M_n$ lässt sich eindeutig als Produkt $x = rs^2$ schreiben, wobei r quadratfrei ist. Für r gibt es nur konstant viele Möglichkeiten und für s gilt $s \le \sqrt{n}$. Damit ist $|M_n| \in \mathcal{O}(\sqrt{n})$. Für jedes $i \ge 1$ ist die Anzahl der Zahlen aus $\{1, \ldots, n\}$, die durch p_i teilbar sind, kleiner oder gleich n/p_i, denn nur jede p_i-te Zahl ist durch p_i teilbar. Hieraus folgt

$$n \le \sum_{i\ge k} \frac{n}{p_i} + \mathcal{O}(\sqrt{n}) \le \frac{n}{2} + \mathcal{O}(\sqrt{n})$$

Dies ein Widerspruch.

Lösung mittels Primzahldichte: Mit p bezeichnen wir Primzahlen. Nach Satz 2.6 liegen zwischen n und $2n$ bereits $\Theta(n/\log n)$ Primzahlen. Daher ist $\sum_{2^k<p<2^{k+1}} \frac{1}{p} \in \Theta(1/k)$ und damit

$$\sum_{p\le 2^k} \frac{1}{p} \in \Theta(\log k)$$

Es folgt $\sum_{p\le n} \frac{1}{p} \in \Theta(\log\log n)$.

Zu Kapitel 3

3.1. Es gibt $2^{10} = 1024$ Schussfolgen, die alle gleich wahrscheinlich sind. Hiervon ist eine Folge dabei, bei der er nie trifft. Bei zehn Folgen landet er genau einen Treffer und bei $\binom{10}{2} = 45$ Folgen sind es genau zwei. Also verbleiben $1024 - 56 = 968$ Schussfolgen mit mindestens drei Treffern. Die Wahrscheinlichkeit ergibt sich zu $\frac{968}{1024} = \frac{121}{128}$, dies sind nach kaufmännischer Rundung 95%.

3.2. (a) Es gibt insgesamt $2^4 = 16$ verschiedene Möglichkeiten welchen Geschlechts die vier Kinder sein können – von vier Jungen ($jjjj$) bis vier Mädchen ($mmmm$). Damit gibt es vier verschiedene Möglichkeiten (das erstgeborene Kind ist ein Mädchen ($mjjj$), das zweitgeborene ist ein Mädchen ($jmjj$) usw.). Wir erhalten insgesamt:

$$\Pr[\text{genau ein Mädchen}] = 4 \cdot \frac{1}{16} = \frac{1}{4}$$

3.2. (b) Wenn die ersten beiden Geschlechter feststehen, gibt es für das dritte und vierte Kind genau vier Möglichkeiten, es ist deshalb

$$\Pr[\text{erstes und zweites Kind ein Junge}] = \frac{1}{4}$$

3.2. (c) Die Wahrscheinlichkeit, dass genau zwei Kinder männlich sind, ist $\frac{6}{16}$ (es ist $\binom{4}{2} = 6$), die Wahrscheinlichkeit, dass genau drei Kinder männlich sind, beträgt $\frac{4}{16}$ (es ist $\binom{4}{3} = 4$) und die Wahrscheinlichkeit, dass genau vier Kinder männlich sind, ist $\frac{1}{16}$. Insgesamt erhalten wir

$$\Pr[\text{mindestens zwei Kinder männlich}] = \frac{6}{16} + \frac{4}{16} + \frac{1}{16} = \frac{11}{16}$$

3.2. (d)

$$\Pr[\text{alle Kinder weiblich}] = \frac{1}{16}$$

3.3. Wir nehmen an, dass Alice a wählt und Bob b. Die Anzahl der Paare (a, b) mit $a = b$ ist m. Wir zählen jetzt zunächst die Paare mit $|a - b| \leq n$ und $a < b \leq n$. Deren Anzahl ist $\sum_{j=1}^{n-1} j = \frac{n(n-1)}{2}$. Die Anzahl der Paare mit $|a - b| \leq n$ und $a < b$ sowie $n + 1 \leq b \leq m$ ist nun $(m - n)n$. Für $a < b$ ergibt sich eine Mächtigkeit von $\frac{n(n-1)}{2} + (m-n)n$. Die Anzahl $|\{(a, b) \mid a, b \in M \text{ und } |a - b| \leq n\}|$ errechnet sich damit zu

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

Die Anzahl der Paare ist m^2. Also ergibt sich die gesuchte Wahrscheinlichkeit zu $\frac{1+2n}{m} - \frac{n^2-n}{m^2}$.

3.4. Es sei $Q(n)$ die mittlere Zahl der Vergleiche, wenn alle Positionen für das Pivotelement gleich wahrscheinlich sind. Die Lösung lautet $Q(n) = 2(n+1)H_n - 4n$, wobei H_n die n-te harmonische Zahl ist.

Herleitung über Zufallsvariablen: Wir bezeichnen mit π eine Reihenfolge der Pivotelemente. Für $i < j$ sei X_{ij} die 0-1-wertige Zufallsvariable mit $X_{ij}(\pi) =$ „i wird mit j verglichen“. Im Laufe von Quicksort werden i und j maximal einmal verglichen. Damit ist

$$Q(n) = \sum_{1 \le i < j \le n} E[X_{ij}]$$

Es gilt $X_{ij}(\pi) = 1$ genau dann, wenn eines der beiden Elemente i und j als ein frühestes Pivot-Element im Interval $[i, j]$ gezogen wird. Hieraus folgt $E[X_{ij}] = \frac{2}{j-i+1}$; also

$$\begin{aligned} Q(n) &= \sum_{1 \le i < j \le n} \frac{2}{j-i+1} = \sum_{i=1}^{n-1} \sum_{d=1}^{n-i} \frac{2}{d+1} = 2 \sum_{d=1}^{n-1} \frac{n-d}{d+1} \\ &= 2 \sum_{d=2}^{n} \frac{n+1-d}{d} = -2n + 2 \sum_{d=1}^{n} \frac{n+1-d}{d} \\ &= -2n + 2(n+1)H_n - 2n = 2(n+1)H_n - 4n \end{aligned}$$

Herleitung durch Rekursion: Wir benötigen $n-1$ Vergleiche beim Pivotieren. Also gilt $Q(1) = 0$ und für $n \ge 2$:

$$Q(n) = (n-1) + \frac{1}{n} \sum_{i=1}^{n} \big(Q(i-1) + Q(n-i)\big) = (n-1) + \frac{2}{n} \sum_{i=1}^{n} Q(i-1)$$

Hieraus folgt $nQ(n) = n(n-1) + 2\sum_{i=1}^{n} Q(i-1)$. Eine Subtraktion der jeweiligen Seiten für n und $n-1$ liefert:

$$nQ(n) - (n-1)Q(n-1) = 2(n-1) + 2Q(n-1)$$

Wir erhalten:

$$\begin{aligned} nQ(n) &= 2(n-1) + 2Q(n-1) + (n-1)Q(n-1) \\ &= 2(n-1) + (n+1)Q(n-1) \end{aligned}$$

Eine weitere Umformung ergibt nun:

$$\begin{aligned} \frac{Q(n)}{n+1} &= \frac{2(n-1)}{n(n+1)} + \frac{Q(n-1)}{n} = \frac{2(n-1)}{n(n+1)} + \frac{2(n-2)}{(n-1)n} + \frac{Q(n-2)}{n-1} \\ &= \sum_{k=1}^{n} \frac{2(k-1)}{k(k+1)} = 2\left(\sum_{k=1}^{n} \frac{2}{k+1} - \sum_{k=1}^{n} \frac{1}{k} \right) = 2H_n + \frac{4}{n+1} - 4 \end{aligned}$$

3.5. Es sei $Q(n)$ die durchschnittliche Anzahl an Vergleichen, um das k-te Element in π zu finden. Dabei halten wir k fest, und wir bezeichnen mit i, j Werte mit $1 \le i <$

$j \le n$. Im Laufe von Quickselect werden i und j (genau wie bei Quicksort) maximal einmal verglichen. Damit ist

$$Q(n) = \sum_{1 \le i < j \le n} E[X_{ij}]$$

Falls i und j verglichen werden, ist i oder j aktuelles Pivotelement. Der Erwartungswert $E[X_{ij}]$ hängt von der relativen Position von i und j zu k ab. Wir unterscheiden drei Fälle.

1. Fall: Für $i < j \le k$ gilt $X_{ij}(\pi) = 1$ genau dann, wenn eines der beiden Elemente i und j als ein frühestes Pivot-Element im Interval $[i, k]$ gezogen wird. Hieraus folgt $E[X_{ij}] = \frac{2}{k-i+1}$; und damit ergibt sich:

$$\begin{aligned}\sum_{1 \le i < k} \sum_{i < j \le k} E[X_{ij}] &= 2 \sum_{1 \le i < k} \frac{k-i}{k-i+1} = 2 \sum_{1 \le i < k} \left(1 - \frac{1}{k-i+1}\right) \\ &= 2(k - H_k) < 2(k - \ln k)\end{aligned}$$

2. Fall: Für $k \le i < j$ folgt vollkommen analog

$$\sum_{k < j \le n} \sum_{k \le i < j} E[X_{ij}] = 2(n - k - H_{n-k}) < 2(n - k - \ln(n-k))$$

3. Fall: Für $i < k < j$ gilt jetzt $E[X_{ij}] = \frac{2}{j-i+1}$. Damit ergibt sich eine etwas kompliziertere Rechnung:

$$\begin{aligned}\sum_{1 \le i < k} \sum_{k < j \le n} E[X_{ij}] &= 2 \sum_{1 \le i < k} \sum_{k < j \le n} \frac{1}{j-i+1} \\ &= 2 \sum_{1 \le i < k} \left(\frac{1}{k-i+2} + \cdots + \frac{1}{n-i+1}\right) \\ &< 2 \sum_{1 \le i < k} \left(\ln(n-i+1) - \ln(k-i)\right) = 2 \ln \binom{n}{k-1}\end{aligned}$$

Addieren wir nun die drei Fälle und benutzen $\binom{n}{k-1} < 2^n$, so ergibt sich die Behauptung

$$Q(n) < 2n + 2 \ln \binom{n}{k-1} < 2(1 + \ln 2)n$$

Man kann aus den Rechnungen noch mehr herausholen. Ist k sehr nahe an $n/2$, so ist die Abschätzung bis auf log-Terme genau. Wir erwähnen ohne Beweis $2(1+\ln 2)n \in Q(n) + \mathcal{O}(\log n)$.

3.6. Es gilt $E[X] = \sum_{k=1}^{n} k \Pr[X = k] = n/H_n \sim n/\ln n$. Für die Varianz erhalten wir

$$\mathrm{Var}[X] = \left(\sum_{k=1}^{n} k^2 \Pr[X = k]\right) - n^2/H_n^2 = \frac{H_n \binom{n+1}{2} - n^2}{H_n^2} \sim \frac{n^2}{2 \ln n}$$

Damit strebt die Standardabweichung gegen $\frac{n}{\sqrt{2 \ln n}}$

Zu Kapitel 4

4.1. (a) Sei $f \in C^{(A\times B)}$. Für jedes $a \in A$ definieren wir die Funktion g_a mit $g_a(b) = f(a,b)$. Die zu f gehörige Funktion $\hat{f}$ in $(C^B)^A$ ist dann definiert durch $\hat{f}(a) = g_a$. Man sieht, dass die Zuordnung $f \mapsto \hat{f}$ injektiv ist, denn mit $f(a,b) = (\hat{f}(a))(b)$ kann man die Funktion f rekonstruieren. Umgekehrt sei $\hat{f} \in (C^B)^A$. Dann definiert man $f \in C^{(A\times B)}$ durch $f(a,b) = (\hat{f}(a))(b)$. Also ist die Zuordnung surjektiv.

4.1. (b) Für $f \in C^{A\cup B}$ sei $\hat{f} = (f|_A, f|_B)$ das Paar der beiden Einschränkungen von f auf A und B. Dann ist $f \mapsto \hat{f}$ eine Bijektion von $C^{A\cup B}$ nach $C^A \times C^B$. Dabei lässt sich aus einem Paar (f_1, f_2) die Funktion rekonstruieren, da $A \cap B = \emptyset$ gilt und man somit

$$f(x) = \begin{cases} f_1(x) & x \in A \\ f_2(x) & x \in B \end{cases}$$

als zu (f_1, f_2) gehörige Funktion finden kann.

4.1. (c) Wir wollen einen Widerspruch erzeugen und gehen davon aus, dass $f : A \to 2^A$ eine surjektive Abbildung ist. Dann betrachten wir die Menge $B = \{a \in A \mid a \notin f(a)\}$. Da f surjektiv ist, gibt es ein $b \in A$ mit $f(b) = B$. Wie man die Sache auch dreht und wendet, es ergibt sich ein Widerspruch:

$$b \in B \Leftrightarrow b \in f(b) \Leftrightarrow b \notin B$$

Die erste Äquivalenz ist die Definition von b, die zweite ergibt sich aus der Definition von f.

4.2. Verteile 9 Stellen für die Zahlen auf die 10 Ziffern, wobei die Ziffer 0 immer getroffen wird und keine Ziffer zweimal getroffen wird. Wir erhalten als gesuchte Zahl $\frac{10!}{(10-9)!} - 9! = 10! - 9! = 3265920$.

4.3. (a) Es müssen 4 der 15 Frauen und unabhängig davon 4 der 12 Männer ausgewählt werden. Dafür gibt es $\binom{15}{4}\binom{12}{4} = 1365 \cdot 495 = 675\,675$ Möglichkeiten.

4.3. (b) Es gibt $\binom{15}{8} + \binom{15}{7}\binom{12}{1} = 6435 + 6435 \cdot 12 = 83\,655$ Möglichkeiten, dass *maximal ein* Mann dabei ist. Daher gibt es $\binom{15+12}{8} - 83\,655 = 2\,136\,420$ Möglichkeiten, dass mindestens zwei Männer in der Kommission sind.

4.3. (c) Es gibt $\sum_{i=5}^{8} \binom{12}{i}\binom{15}{8-i} = 792 \cdot 455 + 924 \cdot 105 + 792 \cdot 15 + 495 \cdot 1 = 469\,755$ Möglichkeiten, dass mindestens 5 Männer enthalten sind.

4.4. Es gibt 81 Wörter der Länge 4 über dem Alphabet $\{b, s, w\}$. Jedem Wort ordnen wir ein Muster zu, indem wir die Seiten im Uhrzeigersinn lesen. Wörter bilden nur dann das gleiche Muster, wenn die Wörter zyklische Vertauschungen sind, aber nicht jede der vier zyklischen Vertauschungen liefert ein neues Wort.

Die Wörter, in denen nur jeweils ein Buchstabe vorkommt, entsprechen genau den drei Mustern, bei denen alle Seiten gleich sind. Es gibt ebenfalls drei Muster,

bei denen genau die gegenüberliegenden Seiten gleich sind. Jedem dieser Muster entsprechen zwei Wörter. Es verbleiben 72 Wörter, deren zyklische Vertauschung der Buchstaben jeweils ein neues Wort ergibt. Also gibt es insgesamt $24 = 72/4 + 6/2 + 3 = 18 + 3 + 3$ verschiedene Muster.

4.5.

$$\underbrace{\sum_{i \text{ gerade}} \binom{n}{i}}_{\substack{\text{Anzahl Teilmengen mit} \\ \text{gerade vielen Elementen}}} - \underbrace{\sum_{i \text{ ungerade}} \binom{n}{i}}_{\substack{\text{Anzahl Teilmengen mit} \\ \text{ungerade vielen Elementen}}} = \sum_i \binom{n}{i}(-1)^i = (1-1)^n = 0$$

4.6. (a) Wir wollen von n weißen Objekten einen Teil rot färben und m Objekte blau färben. Eine Vorgehensweise um eine solche Färbung zu erhalten, ist m Objekte blau zu färben. Von den verbleibenden $n - m$ Objekten färben wir einen Teil rot. Es gibt $\binom{n}{m} \cdot 2^{n-m}$ Möglichkeiten, auf diese Weise eine geeignete Färbung zu erzeugen. Eine andere Vorgehensweise ist, einen Teil der weißen Objekte rot zu färben und m der roten Objekte blau zu färben. Die Anzahl hierfür ist $\sum_k \binom{k}{m}\binom{n}{k}$. (Falls weniger als m Objekte rot gefärbt wurden, liefert dies 0 Möglichkeiten, um m davon blau zu färben.) Da beide Vorgehensweisen eindeutig eine gültige Färbung erzeugen, gilt die Behauptung.

4.6. (b) Zweimalige Anwendung des Binomialsatzes liefert

$$((x+1)+1)^n = \sum_k \binom{n}{k}(x+1)^k = \sum_k \binom{n}{k}\sum_\ell \binom{k}{\ell}x^\ell = \sum_{k,\ell}\binom{n}{k}\binom{k}{\ell}x^\ell$$

Ableiten nach x und Einsetzen von $x = 1$ ergibt die Behauptung.

4.6. (c)

$$\sum_i \sum_j \binom{n}{i}\binom{n+i}{j} = \sum_i \binom{n}{i}\sum_j \binom{n+i}{j} = \sum_i \binom{n}{i}2^{n+i}$$
$$= 2^n \sum_i \binom{n}{i}2^i = 2^n(2+1)^n = 6^n$$

4.6. (d) Um $2n+1$ Elemente aus der Menge $M = \{0, \ldots, 2m\}$ auszuwählen gibt es $\binom{2m+1}{2n+1}$ Möglichkeiten. Wir können diese Möglichkeiten auch auf eine alternative Weise zählen. Zuerst wählen wir das mittlere Element einer $2n+1$-elementigen Teilmenge von M und nennen es $m-k$ mit $k \in \mathbb{Z}$. Dann sind links bzw. rechts von $m-k$ noch jeweils genau $m-k$ bzw. $m+k$ Elemente in $\{0, \ldots, 2m\}$ vorhanden. Also gibt es $\binom{m-k}{n}\binom{m+k}{n}$ Möglichkeiten jeweils n davon auszuwählen. Die Summe über alle k liefert nun die Gleichung.

4.6. (e)

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

Die letzte Gleichung ergibt sich aus einer *Teleskopsumme*, da sich Summanden in der vorletzten Zeile wechselseitig aufheben. Ein bijektiver Beweis der Aussage ist auch möglich; als kombinatorische Interpretation der beiden Seiten können dann die nichtkonstanten Abbildungen von $\{1,\dots,m+1\}$ nach $\{1,\dots,n+1\}$ verwendet werden.

4.7. (a) Wir zeigen die Identität für $n \geq -1$, denn für $n = -1$ ist sie trivial, und für $n = 0$ folgt sie wegen $F_1 = \binom{0}{0} = 1$. Sei jetzt $n \geq 1$.

$$\begin{aligned}\sum_{k\leq n}\binom{n-k}{k} &= \sum_{k\leq n-1}\binom{n-k}{k} \\ &= \sum_{k\leq n-1}\left[\binom{n-k-1}{k} + \binom{n-k-1}{k-1}\right] \\ &= \sum_{k\leq n-1}\binom{n-k-1}{k} + \sum_{k\leq n-1}\binom{n-k-1}{k-1} \\ &\overset{\text{Indexversch.}}{=} \sum_{k\leq n-1}\binom{n-k-1}{k} + \sum_{k\leq n-2}\binom{n-k-2}{k} \\ &\overset{\text{Induktion}}{=} F_n + F_{n-1} = F_{n+1}\end{aligned}$$

4.7. (b) Sei $M = \left(\begin{smallmatrix}0 & 1\\ 1 & 1\end{smallmatrix}\right)$ und E die (2×2)-Einheitsmatrix. Wir erinnern uns, dass für die n-te Potenz von M gilt $M^n = \left(\begin{smallmatrix}F_{n-1} & F_n\\ F_n & F_{n+1}\end{smallmatrix}\right)$. Außerdem gilt $M^2 = \left(\begin{smallmatrix}1 & 1\\ 1 & 2\end{smallmatrix}\right)$, d. h. $M^2 = M + E$. Mit dem Binomialsatz 4.3 erhalten wir die n-te Potenz $M^{2n} = (M+E)^n = \sum_i \binom{n}{i} M^i$. Insbesondere sind die oberen rechten Einträge gleich und es folgt die Behauptung.

4.7. (c) Seien M und E die Matrizen aus Teilaufgabe (4.7. (b)). Nun gilt $M^3 = \left(\begin{smallmatrix}1 & 2\\ 2 & 3\end{smallmatrix}\right)$, d. h. $M^3 = 2M + E$. Damit erhalten wir $M^{3n} = (2M+E)^n = \sum_i \binom{n}{i} 2^i M^i$. Betrachten der Einträge der oberen rechten Ecken liefert die Behauptung.

4.7. (d) Seien M und E die Matrizen aus Teilaufgabe (4.7. (b)). Dort hatten wir uns bereits überzeugt, dass $M^2 = M + E$ gilt, also ist $E = M^2 - M$. Damit gilt $E = E^n = (M^2 - M)^n = \sum_j \binom{n}{j}(-M)^j (M^2)^{n-j} = \sum_j \binom{n}{j}(-1)^j M^{2n-j}$. Wir betrachten die

rechten oberen Einträge und erhalten $0 = \sum_j \binom{n}{j}(-1)^j F_{2n-j}$. Nach einer Indexverschiebung mit $j = n - i$ erhalten wir $0 = \sum_i \binom{n}{i}(-1)^{n-i} F_{n+i}$. Nach Kürzen mit $(-1)^{n-2i}$ ergibt sich die Behauptung.

4.8. Sei $A \subseteq \{1, \ldots, n\}$ eine Menge mit $|A| = 3$. Dann ist $\mathrm{sum}(A)$ genau dann gerade, wenn (i) A drei gerade Zahlen enthält oder (ii) A zwei ungerade Zahlen und eine gerade Zahl enthält. Die Menge $\{1, \ldots, n\}$ enthält genau $\lfloor n/2 \rfloor$ gerade Zahlen und $\lceil n/2 \rceil$ ungerade Zahlen. Also gilt

$$G^{(3)}(n) = \binom{\lfloor n/2 \rfloor}{3} + \lfloor n/2 \rfloor \binom{\lceil n/2 \rceil}{2}$$

4.9. (a) Wir betrachten eine Partition der Menge $\{1, \ldots, n+1\}$ in $m+1$ Klassen. Die Klasse, welche das Element $n+1$ enthält, sei ausgezeichnet. Die restlichen Klassen der Partition enthalten zusammen k Elemente. Es gibt $\binom{n}{k}$ Möglichkeiten, diese aus der Menge $\{1, \ldots, n\}$ zu wählen, und für jede dieser Möglichkeiten gibt es $\left\{ {k \atop m} \right\}$ Möglichkeiten diese k Elemente auf m Klassen zu verteilen.

4.9. (b) Sei π eine Permutation von $\{1, \ldots, n\}$ mit k Zykeln. Wir zeichnen einen dieser Zykel speziell aus. Für diese Auswahl gibt es k Möglichkeiten. Nun kodieren wir die restlichen $k-1$ Zykel in einen einzigen Zykel. Dafür werden die $k-1$ nicht markierten Zykel von π so angeordnet, dass deren kleinstes Element vorne steht. Dann werden diese $k-1$ Zykel absteigend nach ihrem kleinsten Element sortiert. Diese Anordnung bestimmt nun den zweiten zur Verfügung stehenden Zykel. Dabei wird der Beginn dieser Sortierung vom Element $n+1$ bestimmt.

Beispiel: Wir wählen $n = 7$ und $\pi = (12)(537)(64)$ und markieren den Zykel (12). Dann ergibt sich als Anordnung der Zykel (375) und (46). Da das kleinste Element des ersten Zykels mit 3 kleiner ist als das kleinste des Zykels (46) mit 4 ergibt sich der Zykel (846375). Der Beginn wird hier mit $n+1 = 8$ kodiert, das Ende des ersten Zykels (46) erkennt man, da die darauffolgende 3 kleiner ist als das kleinste vorherige Element, diese jedoch die jeweils kleinsten Elemente des Zykels sind.

4.9. (c) Diese Aufgabe lässt sich analog zu Teilaufgabe 4.9. (b) lösen. Anstatt nur einen der Zykel zu markieren, werden nun m von k Zykeln markiert. Es gibt $\binom{k}{m}$ Möglichkeiten für diese Markierung. Die restlichen Zykel werden wie eben zusammen mit dem Element $n+1$ in den letzten zur Verfügung stehenden Zykel kodiert.

4.10. (a) Die Schlümpfe kennen natürlich alle Ausweisnummern aller hundert Schlümpfe auswendig. Sie ordnen jeder Ausweisnummer zufällig eine eindeutige Zahl aus dem Bereich 1 bis 100 zu. Diese Zuordnung prägen sich die Schlümpfe rasch ein. Sie ändern ihren Namen auf diese Zahl und wenn sie irgendeinen Ausweis sehen, kennen sie sofort den zugehörigen (neuen) Namen. Sie sind nämlich wirklich ziemlich schlau.

Wenn der Schlumpf mit dem Namen i den Schubladenraum betritt, tut er das Folgende. Er beginnt die Suche nach seinem Ausweis in der Schublade i. Findet er dort seinen Ausweis, so ist er fertig. Ansonsten findet er dort einen Ausweis zu dem der Name j gehört. Als Nächstes schaut dieser Schlumpf dann in der Schublade j nach seinem Ausweis. Findet er dort nicht seinen Ausweis, so erkennt er dennoch einen Namen k, der zum Ausweis gehört. Also wendet er sich der Schublade k zu. Dieses Verfahren wird solange wiederholt bis in 50 Schubladen geschaut wurde oder der korrekte Ausweis gefunden wurde. Eine Zuordnung der Ausweise in die Schubladen wurde vom König festgelegt, der hat natürlich versucht, es den Schlümpfen schwer zu machen. Aber er hatte keine Chance, denn die Zuordnung der Ausweise zu Namen war zufällig. Es ist irrelevant, wie die Ausweise auf die Schubladen verteilt wurden. Wir können uns vorstellen, dass die Zuordnung der Schubladennummern zu Namen eine Zufallspermutation π der Menge $\{1,\dots,100\}$ ist.

Der Schlumpf i wird mit diesem Verfahren mit Sicherheit dann seinen Ausweis sehen, wenn i in einem Zykel von π mit Länge kleiner als 51 liegt. Damit sind die Schlümpfe genau dann erfolgreich, falls es in π keinen Zykel der Länge größer als 50 gibt.

Wir setzen $n = 100$ und berechnen die Wahrscheinlichkeit, dass ein Zykel der Länge größer als $n/2$ bei einer Zufallspermutation auftritt. Gibt es einen solchen, so ist er eindeutig bestimmt, denn es kann keine zwei verschiedenen Zykel dieser Länge geben. Wir betrachten zuerst die Anzahl der Permutationen, die einen Zykel der Länge k für $k > n/2$ haben. Es gibt $\binom{n}{k}$ Möglichkeiten für die Trägermenge dieses Zykels. Bei fester Trägermenge gibt es $(k-1)!$ verschiedene Zykel. Für jeden so gewählten Zykel Z gibt es damit genau $(n-k)!$ Permutationen, die den Zykel Z enthalten, denn die außerhalb von Z liegenden $n-k$ Elemente können beliebig permutiert sein. Insgesamt ergibt sich also die Wahrscheinlichkeit, einen Zykel mit mehr als $n/2$ Elementen zu finden, zu:

$$\frac{1}{n!}\sum_{k=\frac{n}{2}+1}^{n}\binom{n}{k}(k-1)!(n-k)! = \sum_{k=\frac{n}{2}+1}^{n}\frac{1}{k} < \int_{n/2}^{n}\frac{1}{t}\,\mathrm{d}t = \ln 2 \approx 0{,}69$$

Tatsächlich liegt bei 100 Schlümpfen die Wahrscheinlichkeit, dass alle ihren Ausweis finden bei etwa 31,2%. Fortes fortuna adiuvat: den Tüchtigen hilft das Glück! So kamen die Schlümpfe wieder frei.

4.10. (b) Die hier vorgestellte Lösung ist von Eugene Curtin und Max Warshauer [10]. Die Folge der Ausweise in den geöffneten Schubladen legt den Ablauf des Spiels eindeutig fest. Sei $n_1,\dots,n_{100}$ die Folge der Ausweise. Sei $n_{i_1} = 1$. Dann hat Schlumpf 1 die Schubladen $n_1,\dots,n_{i_1}$ geöffnet. Sei $j_2 = \min(\{1,\dots,100\} \setminus \{n_1,\dots,n_{i_1}\})$. Dann ist als Zweites der Schlumpf j_2 dran. Sei $n_{i_2} = j_2$. Der Schlumpf j_2 öffnet die Schubladen $n_{i_1+1},\dots,n_{i_2}$. Als Drittes ist $j_3 = \min(\{1,\dots,100\} \setminus \{n_1,\dots,n_{i_2}\})$ dran, welcher die Schubladen $n_{i_2+1},\dots,n_{i_3}$ mit $n_{i_3} = j_3$ öffnet, und so fort. Dies

definiert die Zykeldarstellung

$$(n_1, \ldots, n_{i_1})\,(n_{i_1+1}, \ldots, n_{i_2}) \cdots (n_{i_k+1}, \ldots, n_{100})$$

einer Permutation. Wenn der König die Ausweise zufällig verteilt, dann ist hier jede Permutation (unabhängig von der Strategie der Schlümpfe) gleich wahrscheinlich. Die Schlümpfe kommen frei, wenn die Permutation keinen Zykel der Länge 51 oder mehr enthält. Die Wahrscheinlichkeit hierfür haben wir oben ausgerechnet. Sie ist genau $1 - H_{100} + H_{50} = 0{,}3118278\cdots$. Die Schlümpfe können also beim modifizierten Spiel höchstens mit dieser Wahrscheinlichkeit entkommen; damit können sie auch im ursprünglichen Spiel nicht mit einer höheren Wahrscheinlichkeit frei kommen. Genauer zeigt dies, dass die in der Lösung von Aufgabe 4.10. (a) erläuterte Strategie optimal ist.

4.11. (a) Es gilt $R = \{i \in \{1, \ldots, n\} \mid R \cap \{i\} \neq \emptyset\}$, Bob stellt also für jedes $i \in \{1, \ldots, n\}$ die Frage „Ist $R \cap \{i\} = \emptyset$?“

4.11. (b) Wir können eine Strategie als binären Entscheidungsbaum auffassen. Dabei entsprechen innere Knoten einer Frage, Verzweigungen dem Ausgang der entsprechenden Frage und die Blätter entsprechen den Antworten Bobs. Der Baum einer Strategie, die mit t Fragen auskommt, kann höchstens 2^t Blätter besitzen.

Alice hat 2^n verschiedene Möglichkeiten R zu wählen. Angenommen, Bob hat eine Gewinnstrategie, die mit $t < n$ Fragen auskommt. Dann muss es Mengen $R_1 \neq R_2$ geben, die im Baum zum selben Blatt führen. Für mindestens eine der beiden Mengen ist Bobs Antwort dann falsch. Dies ist ein Widerspruch zur Korrektheit der Gewinnstrategie.

4.11. (c) Ja! Bob kann durch Fragen „Ist $R \cap \{i\} = \emptyset$?“ für $1 \leq i < n$ die Menge R bis auf das Element n bestimmen. Hier muss er raten. Er gewinnt dann mit Wahrscheinlichkeit $1/2$. Diesen Erwartungswert kann er nicht verbessern, denn sein Strategiebaum aus der Lösung zu Aufgabe 4.11. (b) hat nach $n-1$ Fragen höchstens 2^{n-1} Blätter. Auf diese verteilen sich 2^n Teilmengen, also im Mittel 2 pro Blatt. Fairness sagt, Alice und Bob können bei $r = n - 1$ genauso gut eine Münze werfen.

4.12. (a) Einsetzen der Definition von $C_n = \frac{1}{n+1}\binom{2n}{n}$ und Umordnen der Terme ergibt die gleichwertige Behauptung $\binom{2n}{n+1} = \frac{n}{n+1}\binom{2n}{n}$. Diese widerum folgt aus

$$\binom{2n}{n+1} = \frac{(2n)^{\underline{n+1}}}{(n+1)n!} = \frac{n}{n+1}\frac{(2n)^{\underline{n}}}{(n+1-1)!} = \frac{n}{n+1}\binom{2n}{n} \tag{B.5}$$

4.12. (b) Aus $\binom{n}{k} = \binom{n}{n-k}$ und der Vandermonde'schen Identität folgt

$$\sum_k \binom{n}{k}^2 = \sum_k \binom{n}{k}\binom{n}{n-k} = \binom{2n}{n} = (n+1)C_n$$

4.12. (c) Mit Gleichung (B.5) aus der vorletzten Teilaufgabe sehen wir

$$(n+2)C_{n+1} = \binom{2n+2}{n+1} \overset{(B.5)}{=} \frac{n+2}{n+1}\binom{2n+2}{n} = \frac{n+2}{n+1}\frac{(2n+2)^{\underline{n}}}{n!}$$
$$= \frac{n+2}{n+1} \cdot \frac{(2n+2)(2n+1)\cdot(2n)^{\underline{n}}}{(n+2)(n+1)\cdot n!} = \frac{2(2n+1)}{n+1}\binom{2n}{n}$$

und damit $C_{n+1} = \frac{2(2n+1)}{n+2}C_n$.

4.13. Sei T_n die Anzahl der Triangulierungen eines regelmäßigen n-Ecks mit der Knotenmenge $\{1,\dots,n\}$ und $n \geq 3$. Damit gilt $T_3 = C_1 = 1$. Sei jetzt $n \geq 4$. Die Kante $\{n,1\}$ ist in jeder Triangulierung an genau einem Dreieck beteiligt. Dieses Dreieck ist durch eine der $n-2$ Ecken k in $\{2,\dots,n-1\}$ spezifiziert. Durch Zerteilen des n-Ecks an dem Dreieck ergibt sich ein k-Eck und ein $(n-k+1)$-Eck die unabhängig voneinander trianguliert werden können. Setzen wir noch $T_2 = 1$, so erhalten wir $T_n = \sum_{k=2}^{n-1} T_k T_{n-k+1} = \sum_{\ell=0}^{n-3} C_\ell C_{n-3-\ell}$ Die zweite Gleichheit ergibt sich mit Induktion und einer Indexverschiebung. Mit Korollar 4.41 folgt $T_n = C_{n-2}$ und damit die Behauptung.

4.14. (a) Im Gegensatz zu einer Antikette ist eine *Kette* eine Folge $K_1,\dots,K_\ell$ mit $K_i \subsetneq K_{i+1}$, und eine maximale Kette entspricht genau einer Permutation $\pi = (\pi(1),\dots,\pi(n))$ mit $K_i = \{\pi(1),\dots,\pi(i)\}$. Ist nun $\mathcal{A}$ eine Antikette und π eine Permutation, so kommt maximal ein Mitglied $M \in \mathcal{A}$ als $K_i = \{\pi(1),\dots,\pi(i)\}$ vor. Umgekehrt, ist $M \in \mathcal{A}$ mit $|M| = k$, so gibt es genau $k!(n-k)!$ Permutationen π, bei denen M vorkommt. Wir erhalten

$$\sum_{M\in\mathcal{A}} |M|!(n-|M|)! \leq n! \tag{B.6}$$

Der Wert $|M|!(n-|M|)!$ wird minimal für $|M| = \lfloor \frac{n}{2} \rfloor$, da dann $\binom{n}{|M|}$ maximal ist. Also folgt $|\mathcal{A}| \cdot \lfloor \frac{n}{2} \rfloor!(n - \lfloor \frac{n}{2} \rfloor)! \leq n!$ und damit die Behauptung. (Kürzen der Gleichung (B.6) mit $n!$ ergibt die sogenannte LYM-Ungleichung $\sum_{M\in\mathcal{A}} \binom{n}{|M|}^{-1} \leq 1$ nach Lubell, Meshalkin und Yamamoto.)

4.14. (b) Die Menge $\binom{\{1,\dots,n\}}{\lfloor n/2 \rfloor}$ ist eine Antikette mit $\binom{n}{\lfloor n/2 \rfloor}$ Elementen.

Zu Kapitel 5

5.1. Die Reihe $f(z) = \sum_{n\geq 0} F_n z^n$ konvergiert absolut für $|z| < \Phi^{-1}$. Es ist $f(z) = \frac{z}{1-z-z^2}$. Setzen wir $z = 1/10$, so erhalten wir den Wert $10/89$.

5.2. (a) Wir gehen analog wie bei den Fibonacci-Zahlen F_n vor. Es ist

$$\begin{aligned} a(z) &= \sum_{n\geq 0} a_n z^n = z + \sum_{n\geq 2} a_n z^n = z + \sum_{n\geq 2} c_1 a_{n-1} z^n + \sum_{n\geq 2} c_2 a_{n-2} z^n \\ &= z + c_1 z a(z) + c_2 z^2 a(z), \end{aligned}$$

also $a(z) = \frac{z}{1-c_1 z - c_2 z^2}$.

5.2. (b) Die Nullstellen des Nenners sind $-\frac{c_1}{2c_2} \pm \frac{1}{c_2}\sqrt{(\frac{c_1}{2})^2 + c_2}$, also $-\frac{\lambda_1}{c_1}$ und $-\frac{\lambda_2}{c_2}$, und sie sind verschieden. Damit erhalten wir durch Partialbruchzerlegung und Koeffizientenvergleich die Form für a_n.

5.3. Wir definieren die erzeugende Funktion $a(z) = \sum_{n\geq 0} a_n z^n$. Es gilt

$$\begin{aligned} a(z) &= 2 + 5z + \sum_{n\geq 2} a_n z^n = 2 + 5z + 5\sum_{n\geq 2} a_{n-1} z^n - 6\sum_{n\geq 2} a_{n-2} z^n \\ &= 2 + 5z - 10z + 5z a(z) - 6z^2 a(z) \end{aligned}$$

Auflösen nach $a(z)$ liefert $a(z) = (2-5z)/(1-5z+6z^2)$. Mit Hilfe von Partialbruchzerlegung erhält man dann $a(z) = 1/(1-2z) + 1/(1-3z)$. Ein Koeffizientenvergleich mit den zugehörigen geometrischen Reihen liefert schließlich die Formel $a_n = 2^n + 3^n$.

5.4. Wir definieren die erzeugende Funktion $a(z) = \sum_{n\geq 0} a_n z^n$. Es gilt

$$\begin{aligned} a(z) &= z + \sum_{n\geq 2} a_n z^n = z + \sum_{n\geq 2} (3a_{n-1} - 2a_{n-2} + 2^{n-1}) z^n \\ &= z + 3z a(z) - 2z^2 a(z) + \frac{2z^2}{1-2z} \end{aligned}$$

Auflösen nach $a(z)$ liefert $a(z) = z/\big((1-3z+2z^2)(1-2z)\big)$. Mit Hilfe einer Partialbruchzerlegung erhält man daraus $a(z) = 1/(1-z) + 1/(1-2z)^2 - 2/(1-2z)$. Wir benutzen die Formel $\sum_{n\geq 0}(n+1)z^n = 1/(1-z)^2$ für $|z| < 1$, die sich durch Ableiten der geometrischen Reihe ergibt. Zusammen mit der Summenformel für die geometrische Reihe erhalten wir

$$a(z) = \sum_{n\geq 0} z^n + \sum_{n\geq 0} (n+1) 2^n z^n - 2\sum_{n\geq 0} 2^n z^n$$

Ein Koeffizientenvergleich liefert wie gewünscht $a_n = 1 + (n-1)2^n$.

5.5. Es gilt:

$$h(z) = \sum_{n\geq 0}\sum_{k=1}^{n} z^n/k = \left(\sum_{n\geq 1}\sum_{k=1}^{n-1} z^n/k\right) + \sum_{n\geq 1} z^n/n = z h(z) - \ln(1-z)$$

Hieraus folgt $h(z) = \frac{\ln(1-z)}{z-1}$.

5.6. 1. *Standardlösung*: Setze $G_n = F_{2n}$, damit $G_0 = 0$ und damit $G_1 = F_2 = 1$. Für $n \geq 2$ erhalten wir $G_n = 3G_{n-1} - G_{n-2}$, denn $F_{2n+2} = 2F_{2n} + F_{2n-1}$ und $F_{2n} = F_{2n-1} + F_{2n-2}$, also ist $F_{2n-1} = F_{2n} - F_{2n-2}$ und damit $F_{2n+2} = 3F_{2n} - F_{2n-2}$. Sei $g(z)$ die erzeugende Funktion der Fibonacci-Zahlen G_n mit geradem Index. Dann gilt

$$\begin{aligned} g(z) &= z + \sum_{n\geq 2} G_n z^n = z + 3\left(\sum_{n\geq 2} G_{n-1} z^n\right) - \left(\sum_{n\geq 2} G_{n-2} z^n\right) \\ &= z + 3zg(z) - z^2 g(z) \end{aligned}$$

Hieraus folgt $g(z) = z/(z^2 - 3z + 1)$.

2. *Alternativlösung mit Magie*: Sei $f(z) = z/(1 - z - z^2)$ die erzeugende Funktion der Fibonacci-Zahlen. Betrachte die Funktion $h(z) = f(z) + f(-z)$. Es gilt $h(z) = \sum_{n\geq 0} F_n(z^n + (-1)^n z^n) = 2\sum_{n\geq 0} F_{2n}(z^2)^n$ Damit ist $g(z) = \frac{h(\sqrt{z})}{2}$ also die erzeugende Funktion der Fibonacci-Zahlen mit geradem Index. Es ist

$$\begin{aligned} h(\sqrt{z}) &= \sqrt{z}\left(\frac{1}{1-\sqrt{z}-z} - \frac{1}{1+\sqrt{z}-z}\right) \\ &= \sqrt{z}\left(\frac{2\sqrt{z}}{(1-z)^2 - (\sqrt{z})^2}\right) = \frac{2z}{z^2 - 3z + 1} \end{aligned}$$

Damit ergibt sich erneut $g(z) = \frac{h(\sqrt{z})}{2} = z/(z^2 - 3z + 1)$.

5.7. Wir definieren die erzeugende Funktion $a(z) = \sum_{n\geq 0} a_n z^n$. Zunächst beobachten wir, dass $\sum_{i=0}^{n}(n-i)a_i$ für $n > 0$ genau a_n entspricht und für $n = 0$ den Wert 0 ergibt. Wir stellen $a(z)$ als Faltung mit sich selbst dar:

$$\begin{aligned} a(z) &= \sum_{n\geq 0} a_n z^n = 1 + \sum_{n\geq 0}\sum_{i=0}^{n}(n-i)a_i z^n \\ &= 1 + \left(\sum_{n\geq 0} a_n z^n\right)\left(\sum_{n\geq 0} n z^n\right) = 1 + a(z)\cdot\frac{z}{(1-z)^2} \end{aligned}$$

Es ergibt sich somit $a(z) = \frac{(1-z)^2}{(1-z)^2 - z} = \frac{(1-z)^2}{z^2 - 3z + 1}$.

5.8. Sei $r(z)$ die exponentielle erzeugende Funktion der Rencontres-Zahlen. Nach Satz 4.18 ist bekannt, dass $R_n = n!\sum_{k=0}^{n}\frac{(-1)^k}{k!}$ gilt. Damit erhalten wir

$$r(z) = \sum_{n\geq 0}\frac{R_n}{n!}z^n = \sum_{n\geq 0}\sum_{k=0}^{n}\frac{(-1)^k}{k!}z^n = \left(\sum_{n\geq 0}\frac{(-1)^n}{n!}z^n\right)\left(\sum_{n\geq 0} z^n\right) = \frac{e^{-z}}{1-z}$$

5.9. (a) Da $\delta(q_0, \varepsilon) = q_0$ gilt, folgt

$$\begin{aligned} L_{q_0} &= \{\varepsilon\} \cup \{wa \mid w \in \Sigma^*,\ a \in \Sigma,\ \delta(q_0, wa) = q_0\} \\ &= \{\varepsilon\} \cup \{wa \mid w \in \Sigma^*,\ a \in \Sigma,\ \delta(\delta(q_0, w), a) = q_0\} \\ &= \{\varepsilon\} \cup \bigcup_p \{wa \mid w \in \Sigma^*,\ a \in \Sigma,\ \delta(q_0, w) = p,\ \delta(p, a) = q_0\} \\ &= \{\varepsilon\} \cup \bigcup_{\delta(p,a)=q_0} L_p \cdot a \end{aligned}$$

Für $q \neq q_0$ ist $\delta(q_0, \varepsilon) \neq q$ und damit insbesondere $\varepsilon \notin L_q$. Die Rechnung ist nun ganz analog zu oben, nur ohne das leere Wort.

5.9. (b) Da jedes Wort einen eindeutigen Pfad durch den Automaten definiert, sind die Vereinigungen in 5.9. (a) disjunkt. Es gilt also $a_0^{q_0} = 1$ und $a_0^q = 0$ für $q \neq q_0$ sowie $a_n^q = \sum_{\delta(p,a)=q} a_{n-1}^p$ für alle $q \in Q$ und $n > 0$.

5.9. (c) Die Anzahl der Wörter der Länge n in $L(\mathcal{A})$ ist gerade die Summe $\sum_{q \in F} a_n^q$, denn $L(\mathcal{A}) = \bigcup_{q \in F} L_q$, wobei die Vereinigung disjunkt ist.

5.9. (d) Mit Hilfe der Formeln aus Teil 5.9. (b) erhalten wir folgendes Gleichungssystem:

$$\begin{aligned} a^{q_0}(z) &= 1 + a^{q_0}(z) \cdot z + a^{q_1}(z) \cdot z \\ a^{q_1}(z) &= a^{q_0}(z) \cdot z \end{aligned}$$

Wir müssen $a^{q_2}(z)$ nicht betrachten, da es von q_2 keinen Weg in einen Endzustand gibt. Durch Lösen des Gleichungssystems ergibt sich:

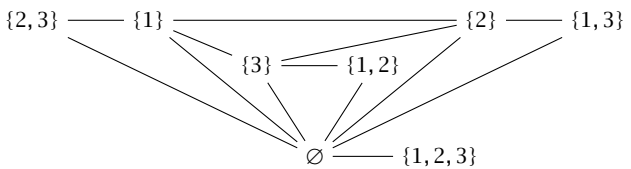
$$a^{q_0}(z) = \frac{1}{1 - z - z^2} \qquad \text{und} \qquad a^{q_1}(z) = \frac{z}{1 - z - z^2}$$

Sei $f(z)$ die erzeugende Funktion der Fibonacci-Zahlen. Dann gilt $f(z) = z \cdot a^{q_0}(z) = a^{q_1}(z)$. Nach Teil 5.9. (c) ist $b(z) = a^{q_0}(z) + a^{q_1}(z) = \sum_{n \geq 0}(F_{n+1} + F_n)z^n = \sum_{n \geq 0} F_{n+2} z^n$ die gesucht erzeugende Funktion. Der Automat akzeptiert also genau F_{n+2} Wörter der Länge n. Dies haben wir bereits in Beispiel 1.25 auf einem anderen Weg berechnet.

Zu Kapitel 6

6.1. Die Menge der Kanten ist eine Teilmenge von $\binom{V}{2}$. Da $|V| = n$ gibt es $2^{\binom{n}{2}}$ solche Teilmengen und somit $2^{\binom{n}{2}}$ Graphen. Man beachte, dass hierbei isomorphe Graphen mehrfach gezählt werden.

6.2. (a)



6.2. (b) Die Anzahl der Knoten ist $|V_n| = 2^n$. Enthält eine Menge i Elemente, so gibt es zu allen Teilmengen der restlichen $n-i$ Elemente Kanten. Dies liefert $\sum_{i=1}^{n} \binom{n}{i} 2^{n-i} = 3^n$ Paare. Hierin ist allerdings noch die Schlinge $\varnothing - \varnothing$ enthalten. Außerdem werden die Kanten doppelt gezählt. Die Anzahl an Kanten ergibt sich damit zu $\frac{3^n - 1}{2}$.

6.3. (a) Sei d_x der Grad von Knoten $x \in V$. Dann gilt $4|V| \leq \sum_{x \in V} d_x = 2|E|$. Daraus folgt $2|V| \leq |E|$.

6.3. (b) Für $n = 5$ erfüllt der vollständige Graph mit 5 Knoten die Behauptung. Sei nun (V, E) ein Graph mit mindestens 5 Knoten, bei dem alle Knoten den Grad 4 haben. Seien $x_1, x_2, y_1, y_2 \in V$ vier verschiedene Knoten mit $(x_1, x_2), (y_1, y_2) \in E$. Wir entfernen die Kanten (x_1, x_2) und (y_1, y_2). Hiernach haben x_1, x_2, y_1, y_2 den Grad 3. Alle anderen Knoten haben den Grad 4. Wir nehmen einen neuen Knoten $z \notin V$ hinzu. Außerdem fügen wir die 4 Kanten (z, x_1), (z, x_2), (z, y_1) und (z, y_2) ein. In dem entstandenen Graphen (V', E') mit $V' = V \cup \{z\}$ und $E' = (E \setminus \{(x_1, x_2), (y_1, y_2)\}) \cup \{(z, x_1), (z, x_2), (z, y_1), (z, y_2)\}$ haben alle Knoten den Grad 4. Dieses induktive Vorgehen zeigt die Behauptung.

6.4. Da G nicht vollständig ist, existieren Knoten $a, b \in V$ mit $ab \notin E$. Da G zusammenhängend ist, gibt es in G einen kürzesten Weg $a = x_1, x_2, \ldots, x_n = b$ mit $n \geq 3$. Zwischen x_1 und x_3 gibt es keine Kante, sonst ließe sich dieser Weg verkürzen. Also gilt die Behauptung mit $(x_1, x_2, x_3) = (u, v, w)$.

6.5. Angenommen G ist nicht zusammenhängend, dann lässt sich die Knotenmenge V in zwei disjunkte, nichtleere Mengen A, B zerlegen, so dass keine Kanten zwischen A und B erlaufen. Wir zeigen jetzt, dass $\overline{G}$ zusammenhängend ist. Seien $u, v \in A$. Es existiert ein Knoten $x \in B$ mit $ux, vx \in \overline{E}$. Die Knoten u und v sind also zusammenhängend. Analog gilt dies für $u, v \in B$. Für $u \in A, v \in B$ ergibt sich direkt $uv \in \overline{E}$.

6.6. Angenommen, es gäbe zwei längste disjunkte einfache Wege $u_0 \cdots u_{\ell(G)}$ und $v_0 \cdots v_{\ell(G)}$ in G. Da G zusammenhängend ist, gibt es zwei Knoten u_i und v_j, so dass ein doppelpunktfreier Weg $u_i = w_0, w_1, \ldots, w_{k-1}, w_k = v_j$ existiert mit $\{w_1, \ldots, w_{k-1}\} \cap \{u_0, \ldots, u_{\ell(G)}, v_0, \ldots, v_{\ell(G)}\} = \emptyset$. Ohne Einschränkung sei $i \geq \ell(G)/2$ und $j \geq \ell(G)/2$, andernfalls nummerieren wir den jeweiligen Weg in der entgegengesetzten Richtung. Dann ist aber die Länge des Weges $u_0, \ldots, u_i, w_1, \ldots, w_{k-1}, v_j, \ldots, v_0$ mindestens $\ell(G)/2 + 1 + \ell(G)/2 > \ell(G)$, ein Widerspruch!

6.7. Für den Grad eines Knotens $x \in V$gilt $0 \leq d_x \leq |V| - 1$. Es sind also $|V|$ verschiedene Werte für d_x möglich. Haben nun alle Knoten einen unterschiedlichen Grad, so muss es insbesondere einen Knoten vom Grad 0 und einen Knoten vom Grad $|V| - 1$ geben. Für $|V| \geq 2$ ist dies nicht möglich, denn der Knoten mit Grad $|V| - 1$ ist mit allen anderen Knoten verbunden.

6.8. Sei G ein zusammenhängender Graph, in dem alle Knoten geraden Grad haben. Der Graph G enthält einen Eulerkreis. Nach Entfernen einer beliebigen Kante existiert noch ein Eulerweg. Insbesondere ist der entstandene Graph zusammenhängend. Der Graph G enthält also keine Brücke.

6.9. Sei $G = (V, E)$ ein gerichteter Graph mit $V = \Sigma^{k-1}$ und beschrifteten Kanten $x_1 \cdots x_{k-1} \xrightarrow{a} x_2 \cdots x_{k-1} a$ für jedes $a \in \Sigma$ (Schleifen sind möglich). Bei jedem

Knoten ist der Ein- und Ausgangsgrad $|\Sigma|$. Der Graph G ist zusammenhängend, denn es gilt $x_1 \cdots x_{k-1} \xrightarrow{y_1} \cdots \xrightarrow{y_{k-1}} y_1 \cdots y_{k-1}$. Es existiert deshalb ein gerichteter Eulerkreis $z_1 \cdots z_\ell z_1$ der jede Kante genau einmal besucht. Auf diesem Kreis kommt bei der Sequenz der Beschriftungen jedes Wort genau einmal vor. Aus $|E| = |\Sigma|^k$ folgt $\ell = |\Sigma|^k$. Sei $y_1 \dots y_\ell$ die Sequenz der Kantenbeschriftungen, dann ist $w = z_1 y_1 \dots y_\ell$ das gesuchte Wort. Man bezeichnet w oft auch als De Bruijn-Folge der Ordnung k (nach Nicolaas Govert de Bruijn, 1918–2012).

6.10. Wir beschreiben den Algorithmus von Carl Hierholzer (1840–1871), welcher posthum erschien [25]. In diesem Verfahren starten wir bei einem beliebigen Knoten v und konstruieren einen Kreis K, indem wir zu dem anfangs leeren Pfad immer weitere Kanten hinzufügen und diese aus dem ursprünglichen Graphen entfernen. Durch die Gradbedingung ist garantiert, dass wir irgendwann wieder zu v zurückkommen. Falls wir keine Kanten mehr hinzufügen können, haben wir also einen geschlossenen Pfad von v nach v gefunden. Sind alle Kanten aus G entfernt, so benutzt K alle Kanten und wir sind fertig. Andernfalls gehen wir den gefundenen Pfad zurück, bis wir auf den ersten Knoten u treffen, der noch ausgehende Kanten hat. Da G zusammenhängend ist, muss u existieren. Von u ausgehend führen wir den Algorithmus rekursiv aus und fügen den rekursiv berechneten Kreis anstelle von u in K ein. Dann laufen wir den entstandenen Kreis weiter zurück (insbesondere laufen wir erst durch den neu eingefügten Teil zurück) und bearbeiten auf die gleiche Weise alle Knoten mit noch ausgehenden Kanten. Am Ende dieses Vorgehens haben wir alle Kanten des ursprünglichen Graphen in den Kreis übernommen, der damit ein Eulerkreis ist. Die Laufzeit ergibt sich dadurch, dass wir in jedem Schritt eine Kante besuchen. Aus dem ursprünglichen Graphen wird nach einem Besuch einer Kante diese aus G gelöscht. Im Kreis K besuchen wir durch ausschließliches Rückwärtslaufen jede Kante maximal einmal. Damit wird jede Kante insgesamt höchstens zweimal betrachtet.

6.11. Für eine beliebige bijektive Funktion $\varphi : E \to \{1, \dots, 12\}$ gilt

$$\sum_{v \in V} \sum_{vw \in E} \varphi(vw) = 2 \cdot \sum_{i=1}^{12} i = 156$$

Bei gleicher Gewichtssumme an allen 8 Ecken, müsste dieses Eckengewicht $156/8 = 19{,}5$ sein, ein Widerspruch!

6.12. Für $n = 0$ und $n = 1$ ist die Äquivalenz trivial erfüllt, da Bäume nicht leer sind und Bäume mit nur einem Knoten keine Kanten haben. Sei also $n \geq 2$.

$\Rightarrow$: Ein Baum mit n Knoten hat $n - 1$ Kanten. Da in der Summe jede Kante genau zweimal gezählt wird, folgt $\sum_{i=1}^{n} d_i = 2n - 2$.

$\Leftarrow$: Für $n = 2$ gilt die Behauptung. Sei $n \geq 3$. Dann existieren $i, j \in \{1, \dots, n\}$ mit $d_i = 1$ und $d_j > 1$. Ohne Einschränkung sei $i = n$ und $j = n - 1$. Durch Induktion existiert ein Baum $(\{1, \dots, n-1\}, E)$, so dass für $1 \leq i \leq n-2$ der Knoten i den Grad d_i hat, und Knoten $n - 1$ hat Grad $d_{n-1} - 1$. Nun ist $(\{1, \dots, n\}, E \cup \{(n - 1, n)\})$ ein Baum, bei dem Knoten i den Grade d_i hat.

6.13. Für $|V| = 1$ und $|V| = 2$ ist die Aussage wahr. Sei nun $|V| > 2$. Die Abbildung φ permutiert die Blätter $B = \{x \in V \mid d_x = 1\}$. Damit ist die Einschränkung $\varphi|_{V\setminus B}$ ein Automorphismus auf dem von $V \setminus B$ induzierten Untergraphen, welcher selbst wieder ein Baum ist. Mit Induktion lässt $\varphi|_{V\setminus B}$ einen Knoten y oder eine Kante e fix. Also lässt auch φ einen Knoten y oder eine Kante e fix.

6.14. Als erstes beobachten wir, dass zwei verschiedene Mengen A_i und A_j durch Entfernen von x genau dann gleich werden, wenn sie sich nur durch x unterscheiden (d. h., die symmetrische Differenz von A_i und A_j ist $\{x\}$). Ohne Einschränkung sei $\ell = n$. Wir konstruieren einen kantengefärbten Graph mit Knotenmenge $\{A_1, \ldots, A_n\}$. Eine Kante zwischen A_i und A_j existiert genau dann, wenn sich A_i und A_j nur um ein Element $k \in M$ unterscheiden. Diese Kante wird mit k gefärbt. Sei A_i ein Knoten auf einem Kreis und k die Farbe einer von A_i ausgehenden Kante e auf diesem Kreis. Dann muss auf diesem Kreis eine weitere Kante mit dieser Farbe existieren (wenn z. B. der Nachbar von A_i auf e das Element k nicht enthält, muss es irgendwann auf diesem Kreis wieder „dazukommen“) . Diese Kante entfernen wir aus dem Graph. Indem wir so sukzessiv Kanten aus dem Graph entfernen, erhalten wir einen Wald (keine Kreise). In diesem Wald kommen alle Farben noch vor, die im ursprünglichen Graph aufgetreten sind. Da ein Wald mit n Knoten höchstens $n - 1$ Kanten besitzt, gibt es eine Farbe x, die in dem ursprünglichen Graph nicht vorgekommen ist. Wenn wir diese Farbe x aus den A_i, $1 \le i \le n$ entfernen, bleiben diese nach obiger Beobachtung weiterhin alle verschieden.

6.15. Ist $P_i = Q_j$, so können wir diese Menge entfernen, daher sind ohne Einschränkung P_i und Q_j paarweise verschieden. Wir bilden einen bipartiten Graphen mit der Knotenmenge $\{P_1, \ldots, P_m\} \cup \{Q_1, \ldots, Q_m\}$ und Kantenmenge $E = \{(P_i, Q_j) \mid P_i \cap Q_j \neq \emptyset\}$. Ein gemeinsames Vertretersystem definiert ein perfektes Matching und umgekehrt. Wir müssen also die Existenz eines perfekten Matchings nachweisen. Hierfür verwenden wir den Heiratssatz 6.11. Zu zeigen ist nur, dass für $S \subseteq \{P_1, \ldots P_m\}$ die Heiratsbedingung $|N(S)| \ge |S|$ erfüllt ist. Für jedes $x \in P_i \in S$ gibt es ein Q_j mit $x \in Q_j \in N(S)$. Also gilt

$$\bigcup_{P_i \in S} P_i \subseteq \bigcup_{Q_j \in N(S)} Q_j$$

Links und rechts stehen disjunkte Vereinigungen von Klassen mit jeweils genau k Elementen, daher ist schließlich $|S| \le |N(S)|$.

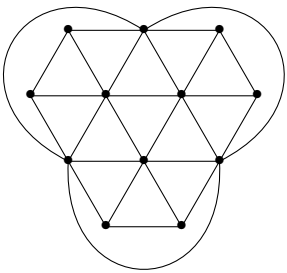
6.16. Angenommen, es gäbe eine stabile Heirat M mit $(a, b'), (a', b) \in M$, in der die Präferenz von a für b' noch niedriger als für b ist. Wir wissen aus der Bemerkung 6.13, dass b im Gale-Shapley-Verfahren seine optimale Partnerin a gefunden hat, folglich muss die Präferenz von b für a' niedriger als für a sein. Es würde also beim Zusammentreffen von den Paaren (a, b') und (a', b) zu einer Scheidung und anschließender neuer Bindung (a, b) kommen. Dies ist ein Widerspruch zur Stabilität von M.

6.17. (a) Aus der Abschätzung $e \leq 3n - 6$ und der Eulerformel $n - e + f = 2$ folgt

$$f = 2 - n + e \leq 2 - n + 3n - 6 = 2n - 4$$

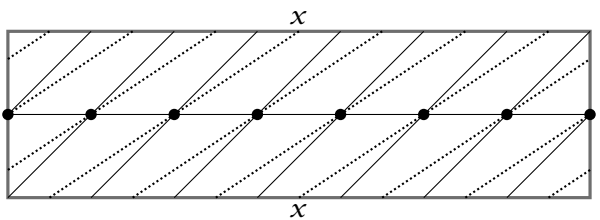
6.17. (b) Die Summe der Knotengrade ist $dn/2 + 2dn/2 = 3dn/2$. Dies liefert $3dn/2 = 2e$ und damit $3dn = 4e$. Mit $e \leq 3n - 6$ folgt $3dn \leq 12n - 24$ und $24 \leq (12 - 3d)n$. Für $d \geq 4$ ist die Ungleichung nicht erfüllt.

6.17. (c)



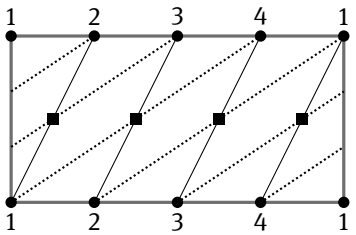
6.18. Zunächst entfernen wir alle Kanten. Dann ist $m = 0$. Für $m = 0$ ist nun $f = 1$ und $n = z$. Fügen wir nacheinander die Kanten wieder ein, so wird jeweils entweder z um 1 verringert und f bleibt gleich oder eine Facette wird zerteilt. Dann bleibt z gleich und f wird um 1 vergrößert.

6.19. Wir betrachten zunächst den Graph K_7. Wir stellen die Torusoberfläche als Rechteck dar, welches wir jeweils entlang der gegenüberliegenden Seiten verkleben. Insbesondere stimmt der obere Punkt x mit dem unteren Punkt x überein, und der Knoten ganz links ist mit dem Knoten ganz rechts identisch.



Die horizontalen Kanten verbinden jeweils nebeneinander liegende Knoten, die durchgezogenen schräg verlaufenden Kanten überspringen einen Knoten und die gestrichelten Kanten überspringen jeweils zwei Knoten. Es gibt keine Kreuzungen und, wie man gut an einem mittleren Knoten erkennt, ist der Grad aller Knoten 6. Damit sind alle Kanten des K_7 vorhanden.

Um den Graph $K_{4,4}$ zu zeichnen, gehen wir ganz analog vor. Die einen vier Knoten $\{1,2,3,4\}$ (rund) zeichnen wir auf den Rand des Rechtecks; insbesondere entsprechen die vier Punkte in den Ecken nur einem einzigen Knoten. Die anderen vier Knoten (eckig) sind in der Mitte des Rechtecks.



Der besseren Übersichtlichkeit wegen haben wir einen Teil der Kanten gestrichelt gezeichnet.

6.20. Nach der Eulerformel gilt in planaren Graphen mit mindestens drei Knoten, dass $|E| \leq 3|V| - 6$. Für den Komplementärgraphen gilt somit

$$\frac{|V|(|V|-1)}{2} - 3|V| + 6 \;\leq\; \left| \binom{V}{2} \setminus E \right| \;\leq\; 3|V| - 6$$

Für $|V| \geq 11$ ist die Ungleichung nicht erfüllt. Also ist jeder Graph mit mehr als 10 Knoten nicht planar oder aber sein Komplementärgraph $\overline{G}$ ist nicht planar. Da es (bis auf Isomorphie) nur endlich viele Graphen mit 10 Knoten oder weniger gibt, folgt die Behauptung.

6.21. Durch Hinzufügen von weiteren Kanten können wir annehmen, dass alle Facetten (auch die äußere) nur von drei Kanten begrenzt werden; dies erhöht den Grad nur. Insbesondere gibt es $2|E|/3$ Facetten. Jeder Knoten x erhält zunächst das Startgewicht $6 - d_x$. Für das Gesamtgewicht gilt $\sum_{x \in V}(6 - d_x) = 6|V| - \sum_{x \in V} d_x = 6|V| - 2|E| = 12$, wobei die letzte Gleichung aus der Eulerformel folgt.

Nun verteilen wir die Gewichte um. Jeder Knoten mit Grad 5 gibt jedem seiner Nachbarn $\frac{1}{5}$ von seinem Gewicht. Da das Gesamtgewicht positiv ist, existiert nach diesem Umverteilen ein Knoten y mit positivem Gewicht. Es gilt $d_y \leq 7$, da zum Startgewicht $6 - d_y$ von y maximal $\frac{d_y}{5}$ hinzu kommen, so dass für das aktuelle Gewicht γ von y die Abschätzung $0 < \gamma \leq 6 - 4d_y/5$ gilt.

Falls $d_y = 7$ gilt, dann hat y mindestens 6 Nachbarn mit Grad 5 (andernfalls hätte y zu wenig abbekommen, um nun positives Gewicht zu haben). Da G triangulliert ist, sind zwei dieser Nachbarn von y durch eine Kante verbunden, wodurch die Aussage in diesem Fall bewiesen ist. Falls $d_y \leq 6$ gilt, dann hat y mindestens einen Nachbarn x mit Grad 5, so dass xy die Forderung der Aufgabe erfüllt.

6.22. (a) Für den leeren Graph gilt die Eigenschaft. Sei $V \neq \emptyset$ und $u \in V$. Wir definieren zwei Teilgraphen durch

$$V_1 = \{v \in V \mid (v,u) \in E\}, \quad E_1 = E \cap (V_1 \times V_1)$$
$$V_2 = \{v \in V \mid (u,v) \in E\}, \quad E_2 = E \cap (V_2 \times V_2)$$

Induktiv seien $a_1 \cdots a_k$ und $b_1 \cdots b_\ell$ einfache Wege in (V_1, E_1) bzw. (V_2, E_2), die jeden Knoten einmal besuchen. Dann ist $a_1 \cdots a_k\, u\, b_1 \cdots b_\ell$ ein einfacher Weg in G, der jeden Knoten einmal besucht.

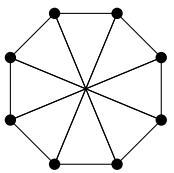
6.22. (b) Wir zeigen die Behauptung mit Induktion. Für $|V| = 2$ ist die Aussage trivial. Sei also $|V| > 2$. Entnehme $x \in V$ und setze $G' = G - x$. Dies bedeutet, $G' = (V', E')$ ist der durch $V' = V \setminus \{x\}$ induzierte Untergraph. Nach Induktion enthält V' einen Knoten y, von dem aus jeder andere Knoten $u \in V'$ in höchstens 2 Schritten erreichbar ist. Ist auch x von y in höchstens 2 Schritten erreichbar, so ist y der gesuchte Knoten. Andernfalls betrachte $u \in V'$ mit $u = y$ oder $(y,u) \in E$. Dann muss $(x,u) \in E$ gelten, ansonsten hätten wir x von y aus in maximal zwei Schritten erreicht. Für alle anderen $v \in V'$, die nicht direkt von y aus erreichbar sind, gibt es ein $u \in V'$ und $(y,u), (u,v) \in E$. Also gilt auch $(x,u), (u,v) \in E$ und v ist von x in zwei Schritten erreichbar. Damit ist x der gesuchte Knoten.

6.23. (a) Wir betrachten die n Schubfächer $\{2i-1, 2i\}$ für $1 \leq i \leq n$. Dadurch wird $\{1, \ldots, 2n\}$ in n Zweiermengen partitioniert. Ein Element x wird in Schubfach S gelegt, falls $x \in S$ gilt. Da wir $n+1$ Elemente aber nur n Schubfächer haben, liegen am Ende in einem Schubfach zwei Elemente. Diese sind benachbart.

6.23. (b) Wir betrachten die Schubfächer $\{i, 2n+1-i\}$ für $1 \leq i \leq n$. Auch hier gehören zwei Elemente aus M zum selben Schubfach.

6.23. (c) Wir betrachten die n Schubfächer $\{u\, 2^s \mid s \geq 0\}$ für alle ungeraden Zahlen $u \in \{1, \ldots, 2n\}$. Seien $k < \ell$ mit $k, \ell \in \{u\, 2^s \mid s \geq 0\}$. Dann unterscheiden sich k und ℓ nur um eine Zweierpotenz, und es gilt $k \mid \ell$.

6.24. (a) Im folgenden Graphen gibt es keine Dreiecke, da der mittlere Punkt in der Zeichnung nicht zum Graphen gehört. Maximale unabhängige Mengen enthalten drei Knoten.



6.24. (b) Es gibt mindestens einen Knoten x vom Grad $d_x \neq 3$, denn sonst wäre $\sum_{x \in V} d_x = 9 \cdot 3$ ungerade, was dem Handschlaglemma widerspricht. Wir unterscheiden nun zwei Fälle. Ist $d_x \geq 4$, dann bilden die 4 Nachbarn von x entweder eine

unabhängige Menge der Größe 4 oder zwei der Knoten bilden mit x zusammen eine Clique der Größe 3. Ist $d_x \leq 2$, dann verbleiben 6 andere Knoten im Graph. Diese 6 Knoten enthalten entweder eine Clique oder eine unabhängige Menge der Größe 3. Enthalten sie eine unabhängige Menge, dann bilden diese 3 Knoten zusammen mit x eine unabhängige Menge der Größe 4.

6.25. Wir definieren eine Färbung b von $\binom{\mathbb{N}}{2}$ durch $b(\{i,j\}) = c(|j-i|)$. Nach dem Satz von Ramsey existiert eine unendliche Teilmenge $X \subseteq \mathbb{N}$, so dass $\binom{X}{2}$ bezüglich b monochromatisch gefärbt ist. Wähle $i,j,k \in X$ mit $i < j < k$ und setze $x = j - i$, $y = k - j$ sowie $z = k - i$. Es ist $z = x + y$ und aus $b(i,j) = b(j,k) = b(i,k)$ folgt $c(x) = c(y) = c(z)$.

6.26. Wir zeigen, dass mit beliebig hoher Wahrscheinlichkeit alle Knoten paarweise zueinander einen Abstand kleiner oder gleich zwei haben, wenn n genügend groß ist. Betrachte zunächst zwei feste Knoten x und y. Wenn n wächst, nimmt die Wahrscheinlichkeit exponentiell ab, dass kein dritter Knoten z vorhanden ist, der sowohl eine Kante zu x als auch zu y hat. Auf der anderen Seite existieren nur quadratisch viele Paare von Knoten. Die Gesamtwahrscheinlichkeit, dass nicht alle Knoten einen Höchstabstand von zwei haben, nimmt also für $n \to \infty$ exponentiell ab.

Zu Kapitel 7

7.1. Sei $\perp$ das kleinste Element. Betrachte zunächst $a \lessdot b$ und $\dim(a) = d$. Dann gibt es eine maximale Kette K von $\perp$ nach a der Länge d und $K \cup \{b\}$ ist eine maximale Kette von $\perp$ nach b. Haben nun je zwei maximale Ketten mit den selben Endpunkten die gleiche Länge, so folgt nach Definition der Dimension $\dim(b) = \dim(a) + 1$.

Für die Rückrichtung betrachte zwei maximale Ketten K_1 und K_2 von c nach b. Die Längen seien jeweils ℓ_i für $i = 1,2$ und wir nehmen $\ell_1 \leq \ell_2$ an. Es sei $d = \dim(c)$ die Dimension von c. Wir zeigen $\dim(b) = d + \ell_1$. Hieraus folgt dann sofort $\ell_1 = \ell_2$, da in jedem Fall $\dim(b) \geq d + \ell_2$ ist.

Für $\ell_1 = 0$ ist die Behauptung klar, da dann $c = b$ sein muss. Sei jetzt $\ell_1 \geq 1$. Die Kette K_1 läuft durch einen vorletzten Punkt a mit $a \lessdot b$, sonst wäre K_1 nicht maximal. Nach Induktion gilt $\dim(a) = d + \ell_1 - 1$. Folgt nun aus $a \lessdot b$ schon $\dim(b) = \dim(a) + 1$, so ist $\dim(b) = d + \ell_1$, wie behauptet.

7.2. (a) Es ist $\Gamma_{b,c}(\perp)(\sigma) = \sigma$ für $b(\sigma) = 0$ und undefiniert für $b(\sigma) = 1$. Also ist $\Gamma_{b,c}(\perp) = \perp$ genau dann, wenn w nirgends terminiert.

7.2. (b) Wähle b und c mit $b(\sigma) = 1$ und $c(\sigma) = \sigma$ für alle $\sigma \in \Sigma$, dann ist $w =$ **while** true **do** id_Σ **od** und $\Gamma_{b,c}(f) = f$. Also sind alle $f \in \mathcal{F}$ Fixpunkte. Insbesondere gilt $\Gamma_{b,c}(\perp) = \perp$ und der Definitionsbereich von $\Gamma_{b,c}(\perp)$ ist leer.

7.2. (c) Aus $w(\sigma) = \tau$ folgt $b(\tau) = 0$. Also ist $w(\sigma) = \sigma$ gleichbedeutend mit $b(\sigma) = 0$. Dies bedeutet $w \sqsubseteq \mathrm{id} \Leftrightarrow \mathrm{dom}(w) = \{\sigma \in \Sigma \mid b(\sigma) = 0\}$. Sei jetzt

$w' =$ **while** b' **do** c **od** und $w \sqsubseteq w'$. Dann ist $w(\sigma) = w'(\sigma)$ für alle $\sigma \in \mathrm{dom}(w)$. Ist also $b(\sigma) = 0$ oder $b'(\sigma) = 0$, so gilt dies für beide. Dies impliziert $b(\sigma) = b'(\sigma)$ für alle $\sigma \in \mathrm{dom}(w)$. Umgekehrt, gilt $b(\sigma) = b'(\sigma)$ für alle $\sigma \in \mathrm{dom}(w)$, so folgt $w \sqsubseteq w'$. Damit gilt $w \sqsubseteq w'$ genau dann, wenn b und b' auf $\mathrm{dom}(w)$ übereinstimmen.

7.2. (d) Terminiert w überall, so ist w überall definiert und aus $w \sqsubseteq f$ folgt $w = f$. Der kleinste Fixpunkt w ist also der einzige Fixpunkt von $\Gamma_{b,c}$. Umgekehrt, sei jetzt $w(\sigma)$ undefiniert. Da c überall definiert ist, gilt dies auch für c^i. Setze $f(c^i(\sigma)) = \sigma$ für alle $i \in \mathbb{N}$ und lasse f undefiniert sonst. Dann ist zunächst $b(c^i(\sigma)) = 1$ für alle $i \in \mathbb{N}$, denn $w(\sigma)$ ist undefiniert. Hieraus folgt $\Gamma_{b,c}(f)(c^i(\sigma)) = f(c^{i+1}(\sigma)) = \sigma = f(c^i(\sigma))$. Es ergibt sich $f \sqsubseteq \Gamma_{b,c}(f)$. Die Kette $f \sqsubseteq \Gamma_{b,c}(f) \sqsubseteq \Gamma^2_{b,c}(f) \sqsubseteq \cdots$ liefert einen Fixpunkt von $\Gamma_{b,c}$, der echt oberhalb von w liegt.

7.2. (e) Sei $c \in \mathcal{F}$ überall undefiniert. Wir können c beispielsweise darstellen durch $c =$ **while** true **do** id_Σ **od**. Wir zeigen, dass $\Gamma_{b,c}$ genau einen Fixpunkt hat. Sei hierfür $\Gamma_{b,c}(f) = f$. Betrachte ein σ mit $b(\sigma) = 0$, dann gilt $\Gamma_{b,c}(f)(\sigma) = \sigma = f(\sigma)$. Für $b(\sigma) = 1$ ist $\Gamma_{b,c}(f)(\sigma) = f(c(\sigma))$ undefiniert, also auch $f(\sigma)$. Damit ist f durch die Bedingung b eindeutig festgelegt.

7.3. Es gibt abzählbar unendliche Verbände, etwa $(\mathbb{N} \times \mathbb{N}, \leq)$, $(\mathbb{Z} \times \mathbb{Z}, \leq)$ oder der Verband (aus der vorigen Aufgabe) aller Teilmengen von $\mathbb{N}$, die entweder endlich sind oder ein endliches Komplement haben. Diese Verbände sind unendlich, aber abzählbar. Potenzmengenverbände haben die Form 2^A. Sie sind also endlich oder überabzählbar. Insbesondere ist jeder abzählbar unendliche Verband ein Beispiel für einen booleschen Verband, der nicht isomorph ist zu einem Potenzmengenverband 2^A für irgendeine Menge A ist.

7.4. In $(\mathbb{Z} \times \mathbb{Z}, \leq)$ ist kein Paar (m, n) irreduzibel, da $(m, n) = (m - 1, n) \vee (m, n - 1)$ gilt. Auch die Hinzunahme eines kleinsten Elements $\perp$ ergibt keine irreduziblen Elemente.

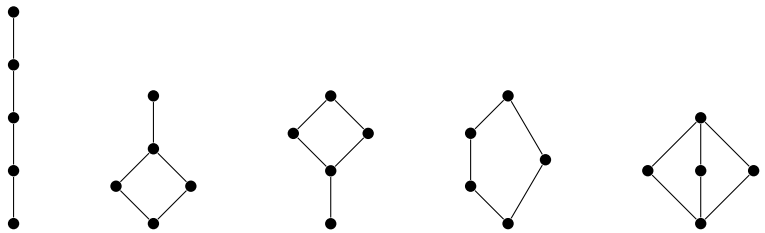
7.5. Sei X unendlich und M der Verband aller Teilmengen von X, die ein endliches Komplement haben. Dann ist M ein Mengenverband, denn es gilt:

1. $A, B \in M \Rightarrow A \cup B \in M$,
2. $A, B \in M \Rightarrow A \cap B \in M$,

Da $A \in M$ unendlich ist, gibt es $a, b \in A$ mit $a \neq b$. Also können wir $A = (A \setminus \{a\}) \cup (A \setminus \{b\})$ schreiben; und A ist nicht irreduzibel.

7.6. Wäre $(2^M, \cup, \cap, 0, 1)$ ein Ring, so wäre $\varnothing = 0$ und $A(A + B) = AA + AB$. Andererseits ist $A(A + B) = A \cap (A \cup B) = A = A \cap A = AA$, also $A \cap B = \varnothing$ für alle $A, B \in 2^M$. Dies widerspricht $M \neq \varnothing$.

7.7.



7.8. M_5 ist nicht distributiv, denn $(a \vee b) \wedge c = c$, aber $(a \wedge c) \vee (b \wedge c) = \bot$. M_5 ist modular: Sei z. B. $a < \top \Rightarrow a \vee (b \wedge \top) = a \vee b = \top = \top \wedge \top = (a \vee b) \wedge \top$. M_5 ist komplementär: Denn z. B. $b \vee c = \top$ und $b \wedge c = \bot$.