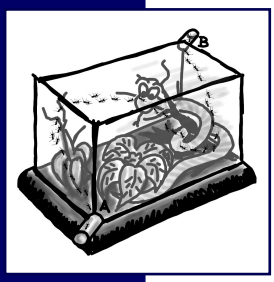
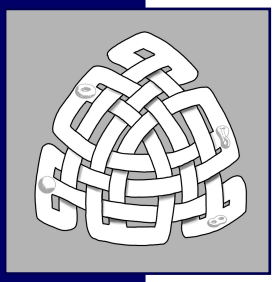
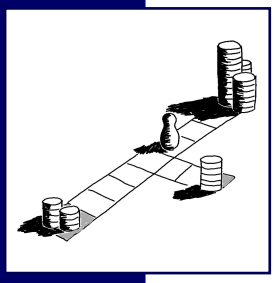
Universität Stuttgart

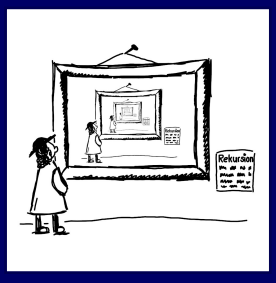
Sieben mathematische Beispielaufgaben

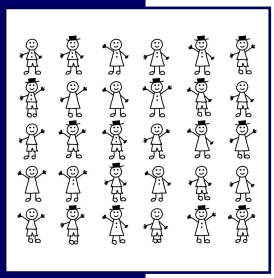
für Studieninteressierte und Schüler:innen der Oberstufe

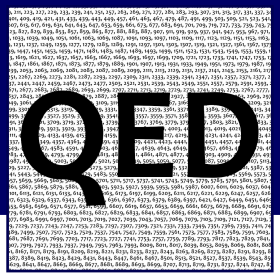












Entwickelt von
Michael Eisermann
Friederike Stoll
Stefan Kohl

Aufgaben mit Lösungen

mathematik
fakultät8

Universität Stuttgart
Fachbereich Mathematik
Pfaffenwaldring 57
70569 Stuttgart

www.f08.uni-stuttgart.de/mathematik

Herzlich willkommen!

Sie interessieren sich für Mathematik? Sie überlegen, vielleicht sogar Mathematik zu studieren? Dann gewinnen Sie mit Hilfe unserer sieben Beispielaufgaben einen eigenen Eindruck über konkrete Inhalte und schöne Themen der Mathematik, mit denen Sie sich im Studium intensiver beschäftigen werden. Die Aufgaben sollen Ihnen helfen, einige Ihrer Fragen zu klären:

- Was ist Mathematik überhaupt?
- Was lernt man im Mathematikstudium?
- Was ist an der Universität anders als in der Schule?

Bitte nehmen Sie sich genügend Zeit, gerne auch Stift und Papier, um unsere Beispielaufgaben zur Mathematik zu lösen. Einige Fragen sind leichter, andere kniffliger. Wenn Sie merken, dass Ihnen die Themen gefallen, Sie viele Aufgaben mit Vergnügen lösen können oder unsere ausführlichen Lösungen nachvollziehen wollen, dann gratulieren wir: ein gutes Zeichen, dass das Studienfach zu Ihnen passt! Sie werden mit Mathematik, so hoffen wir, viel Freude und Erfolg haben.

Für jede Aufgabe erhalten Sie eine Kurzantwort sowie hilfreiche, ausführlichere Informationen:

- Stufe 0: Die Kurzantwort ohne Drumherum, just the facts.
- Stufe 1: Wir erklären, wie Sie die Lösung selbst finden können.
- Stufe 2: Wir erläutern, warum wir diese Aufgabe für interessant halten, wie sie sich in das Mathematikstudium einordnet und welche Erkenntnisse und Techniken sich dahinter verbergen.
- Stufe 3: Zum guten Schluss vertiefen wir einige naheliegende Fragen, Probleme, Beweise, etc.

Wir wünschen Ihnen viel Vergnügen!

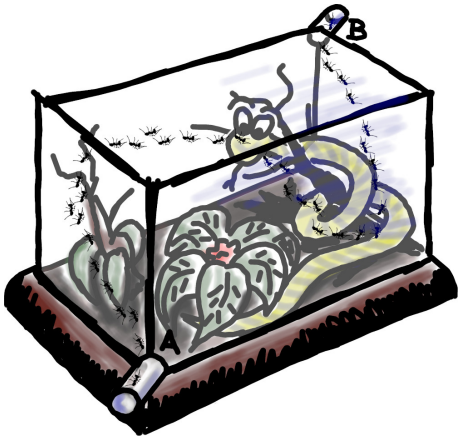
Michael Eisermann
Friederike Stoll
Stefan Kohl

Inhaltsverzeichnis

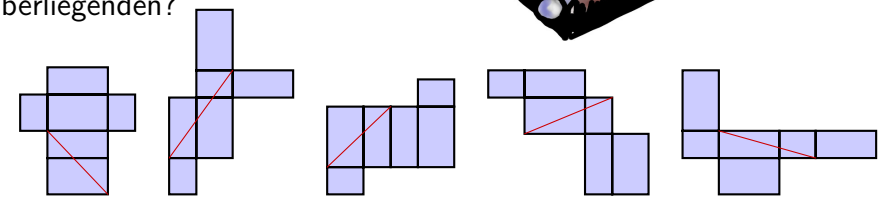
Universität Stuttgart

Beispielaufgabe zur Studienwahl

Mathe macht's kurz: die Ameisenstraße



Ameisen sind dafür bekannt, dass sie ihre Wege optimieren. In einem quaderförmigen Terrarium beobachten Sie eine Ameisenstraße, die auf den Wänden von einer Ecke A (Eingang) zur diagonal gegenüberliegenden Ecke B (Ausgang) verläuft. Wir interessieren uns für kürzeste Wege. Das Terrarium hat innen die Kantenlängen $p = 45$cm, $q = 60$cm, $r = 100$cm. Die Ameisen können auf allen sechs Seiten des Quaders umherlaufen. Welche der folgenden Graphiken sind korrekte Netze der Quaderfläche? Welche der eingezeichneten Wege führen von einer Ecke zur diagonal gegenüberliegenden?



alles korrekt	☐	☐	☐	☐	☐
korrektes Netz, falscher Weg	☐	☐	☐	☐	☐
falsches Netz	☐	☐	☐	☐	☐

Welche Länge L haben die kürzesten Ameisenstraßen von A nach B? ____ cm

Wie lautet die allgemeine Formel für L mit beliebigen Kantenlängen $p \le q \le r$?

☐ $\sqrt{p^2+q^2+r^2}$ ☐ $\sqrt{p^2+q^2+r^2+pqr}$ ☐ $\sqrt{p^2+q^2+r^2+pq}$
☐ $\sqrt{p^2+q^2+r^2+2pq}$ ☐ $\sqrt{p^2+q^2+r^2+2pq+2qr}$ ☐ $\sqrt{p^2+q^2+r^2+2qr}$

Welche Länge K hat der kürzeste Weg von A nach B für eine fliegende Ameise? ____ cm

Wir betrachten eine Quaderfläche Q mit Kantenlängen $0 < p < q < r$.
Wie viele kürzeste Wege gibt es von A nach B in Q? ____

Ameisen finden ihre Wege nicht durch globale vorausschauende Planung, sondern optimieren nur lokal. Sie finden kleine Abkürzungen durch Versuch und Irrtum. Es gibt auf der Quaderfläche mehrere Wege, die lokal minimal sind, sich also lokal durch kleine Veränderungen nicht abkürzen lassen.

Sie können das selbst ausprobieren, indem Sie eine Schnur um einen Karton straff von A nach B spannen. Wie viele lokal minimale Wege gibt es in Q von A nach B? ____

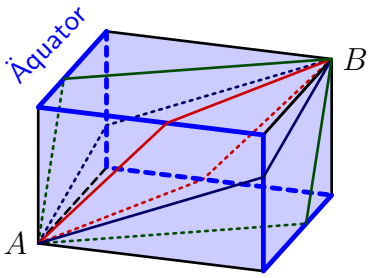
mathematik fakultät8

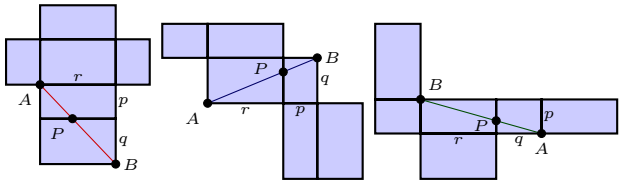
Stufe 0 / Kurzantwort: Die dritte Grafik zeigt kein korrektes Netz eines Quaders. Die zweite Grafik zeigt zwar ein korrektes Netz, aber der Weg verbindet zwei Ecken derselben Seite. Die drei restlichen Grafiken zeigen korrekte Netze und der Weg verbindet diagonal gegenüberliegende Ecken.

Eine kürzeste Ameisenstraße hat die Länge $L = \sqrt{p^2+q^2+r^2+2pq} = 145\text{cm}$. Fliegende Ameisen nehmen die diagonale Luftlinie mit Länge $K = \sqrt{p^2+q^2+r^2} = 125\text{cm}$. Ein Hoch auf Pythagoras!

Auf einem beliebigen Quader mit drei verschiedenen Seitenlängen $p < q < r$ gibt es genau zwei kürzeste Wege. Hingegen gibt es unendlich viele lokal minimale Wege: Für jede natürliche Zahl $n = 0, 1, 2, \ldots$ gibt es einen solchen Weg, der sich $n + 1/2$ mal gleichmäßig um den Quader wickelt.

Stufe 1 / Ausführung: Wir suchen einen möglichst kurzen Weg von A nach B. Anschaulich ist klar, dass dieser Weg über einen Punkt P auf dem „Äquator“ läuft. Dieser besteht aus den sechs Kanten, die nicht an A oder B grenzen. Wir laufen auf geradem Weg von A nach P und dann auf geradem Weg von P nach B. Warum dies tatsächlich so sein muss, klären wir in Stufe 3. Die Äquatorkante, auf der P liegt, grenzt an zwei Flächen an. Auf diesen beiden Flächen verläuft der gesamte Weg von A über P nach B. Wir können den Quader so abwickeln, dass diese beiden Flächen nicht getrennt werden.





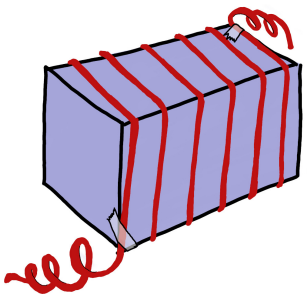
Diese ebenen Netze zeigen: Der Weg kann abgekürzt werden, wenn P nicht auf der geraden Strecke von A nach B liegt. Für jede der sechs Kanten auf dem Äquator finden wir so genau einen Punkt P, über den unser kürzester Weg führen könnte. In der Grafik oben rechts sind diese sechs möglichen Wege abgebildet. Dank Punktsymmetrie sind jeweils zwei davon gleich lang. Jetzt müssen wir also nur noch herausfinden, welche dieser drei Weglängen tatsächlich die kleinste ist.

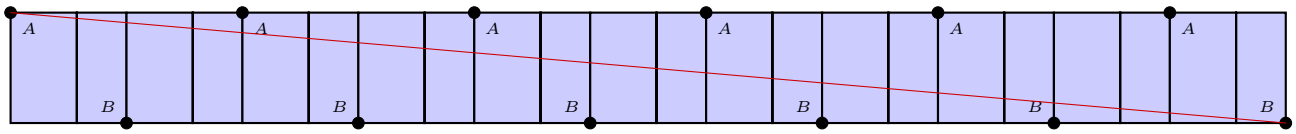
Die drei Längen sind $\sqrt{(p+q)^2+r^2}$, $\sqrt{(p+r)^2+q^2}$ und $\sqrt{(q+r)^2+p^2}$ dank Skizze und Satz von Pythagoras. Welche dieser drei Zahlen ist die kleinste? Bei den konkreten Kantenlängen 45cm, 60cm, 100cm können Sie dies direkt ausrechnen und erhalten $L = 145\text{cm}$.

Wie finden wir die kürzeste der drei Längen allgemein, für beliebige Seitenlängen $p \le q \le r$? Die Längen quadriert sind $(p+q)^2+r^2 = p^2+2pq+q^2+r^2$, $(p+r)^2+q^2 = p^2+2pr+r^2+q^2$ und $(q+r)^2+p^2 = q^2+2qr+r^2+p^2$. Sie unterscheiden sich nur in dem gemischten Summanden $2pq$, $2pr$ bzw. $2qr$, der kleinste davon ist $2pq$, also gilt $L = \sqrt{p^2+q^2+r^2+2pq}$.

Sind alle Seitenlängen verschieden, also $p < q < r$, dann gibt es genau zwei kürzeste Wege. Das gilt auch für $p = q < r$, denn dann ist $pq < pr = qr$. Für $p < q = r$ hingegen gilt $pq = pr < qr$, demnach gibt es vier kürzeste Wege. Auf jedem Würfel, also $p = q = r$, gibt es genau sechs.

Es bleibt die Frage: Wie viele lokal minimale Wege gibt es? Wir finden unendlich viele! Wir geben nicht alle an. Es genügt, unendlich viele Beispiele anzugeben. Zu jeder natürlichen Zahl $n = 0, 1, 2, \ldots$ betrachten wir den Weg, der sich $n + 1/2$ mal gleichmäßig um den Quader wickelt, ähnlich einer Schraubenlinie wie in der Zeichnung rechts angedeutet. Den genauen Verlauf des Weges erhalten wir, indem wir vier Seiten des Quaders wie unten mehrfach abrollen und dann eine Strecke von A nach B einzeichnen. Daran sehen wir auch, dass dieser Weg lokal nicht abgekürzt werden kann.





Stufe 2 / Was will und soll diese Aufgabe?

Nach der Lösung dieser Aufgabe erläutern wir als Rück- und Ausblick, warum wir diese Problemstellung mathematisch interessant finden und inwiefern sie repräsentativ ist für das Mathematikstudium.

Zunächst handelt diese Aufgabe von einer anschaulich-intuitiven Frage: Sie ist mit Schulmathematik leicht zu lösen und erfordert sowohl konkrete Rechnung als auch sorgfältige Überlegung. Dabei nutzen wir allerdings Begriffe und Argumente, die zunächst nur anschaulich begründet sind: Was soll ein Weg sein? Was ist seine Länge? Wie zählen wir Wege? Wie viele kürzeste Wege gibt es?

Anschaulich scheint klar: Wir haben in Stufe 1 alle kürzesten Wege von A nach B gefunden. Aber können wir wirklich sicher sein, dass es mit einem raffinierten Trick nicht noch kürzer geht? Es passiert leider all zu oft, dass sich eine vermeintlich offensichtliche Aussage als falsch entpuppt.

> *Seit man begonnen hat, die einfachsten Behauptungen zu beweisen,*
> *erwiesen sich viele von ihnen als falsch.* (Bertrand Russell)

Bevor wir unser Problem kürzester Wege lösen können, müssen wir es erst sauber formulieren und die Begriffe klären! Diese Grundlagen und sorgsamen Ausführungen behandeln wir in Stufe 3.

Das Problem der kürzesten Wege ist keine exotische Fragestellung, die nur Myrmekologen interessiert, sondern spielt in vielen Bereichen der Mathematik und ihren Anwendungen eine große Rolle.

In der **Analysis** und später in der **Topologie** lernen Sie die nötigen Grundbegriffe wie Abstand und Stetigkeit und beweisen Sätze wie die Dreiecksungleichung oder den Zwischenwertsatz, die wir in Stufe 3 gut gebrauchen können. In der **Geometrie** beschäftigen Sie sich mit Räumen, in denen Sie Längen und Winkel messen können. Damit können Sie insbesondere die Länge eines Weges allgemein definieren und konkret berechnen. Die **Differentialgeometrie** behandelt die zentrale Frage, wie kürzeste Wege aussehen, sogenannte **Geodäten**, die lokal oder gar global die Weglänge minimieren.

Nach Ebene $\mathbb{R}^2$ und Raum $\mathbb{R}^3$ ist die klassische Illustration die Kugeloberfläche, also die Sphäre $\mathbb{S}^2$: Kürzeste Wege sind hier Teile von Großkreisen. Schiffskapitän:innen und Flugzeugpilot:innen nutzen diese, solange keine Hindernisse im Weg liegen. Mit Hindernissen ist lediglich der Raum komplizierter. In der **Geodäsie und Geoinformatik** gehört daher Differentialgeometrie zum Handwerkszeug.

Wir sehen an diesen einfachen Beispielen ein erstaunliches und wichtiges Phänomen: Die Ebene $\mathbb{R}^2$ ist flach, die Winkelsumme in jedem Dreieck ist $180°$. Die Sphäre $\mathbb{S}^2$ hingegen ist gekrümmt: Die Winkelsumme in jedem geodätischen Dreieck ist größer als $180°$. Machen Sie sich eine Skizze! Unsere Quaderfläche Q ist ebenso gekrümmt, die Krümmung sitzt hier jedoch konzentriert in den Ecken. Entlang der Kanten ist Q flach, wie unsere Abwicklungen zeigen. Sie spüren die Krümmung sehr deutlich, wenn Sie versuchen, eine Apfelsinenschale oder eine Pappschachtel flach zu drücken.

Auch die **Physik** nutzt kürzeste Wege, insbesondere in Einsteins Allgemeiner Relativitätstheorie. Die Raumzeit besteht aus drei Raumkoordinaten und einer Zeitkoordinate. Sie ist allerdings nicht flach, sondern wird durch Masse gekrümmt. Im flachen Raum bewegt sich eine Raumsonde auf einer Geraden, allgemein im gekrümmten Raum auf einer Geodäten: Das erklärt die beobachteten, nicht geradlinigen Bahnkurven, und zwar genauer als Newtons klassische Gravitationstheorie!

Ziel der **Optimierung** ist es, die Parameter eines komplexen Systems so zu steuern, dass der Nutzen maximal wird bzw. die Kosten minimal werden. Die Weglänge ist hier ein erstes schönes Beispiel.

Auch in der **Informatik** spielen kürzeste Wege eine Rolle, hier ist das Problem meist diskret oder gar endlich: Gegeben sind endlich viele Punkte und ihre paarweisen Abstände. Gesucht ist ein Algorithmus, der den kürzesten Weg von A nach B bestimmt. Idealerweise soll der Algorithmus nicht nur möglichst exakt, sondern auch schnell sein. Oder würden Sie ein Navigationsgerät kaufen, das erst eine Stunde rechnet, bis es Ihnen einen kurzen Weg vorschlägt?

Stufe 3 / Mathematische Grundlage: Was sind kürzeste Wege und wie finden wir sie?

Wir werden hier einige Definitionen und Sätze aus dem Mathematikstudium kennenlernen und einfache Beweise selbst durchführen. Andere Beweise, die zu aufwändig oder technisch sind, werden wir nur zitieren. Wenn Sie es ganz genau wissen wollen, dann studieren Sie Mathematik!

Wie messen wir euklidische Abstände? Für $n = 1, 2, 3, \ldots$ bezeichnet $\mathbb{R}^n$ die Menge aller n–Tupel $x = (x_1, x_2, \ldots, x_n)$ mit Koordinaten $x_i \in \mathbb{R}$. Für $n = 1$ erhalten wir so die reelle Zahlengerade $\mathbb{R} = \mathbb{R}^1$, für $n = 2$ die reelle Ebene $\mathbb{R}^2$ und für $n = 3$ den reellen Raum $\mathbb{R}^3$. Den Abstand zwischen zwei Punkten $x, y \in \mathbb{R}^n$ berechnen wir mit dem Satz des Pythagoras zu $d(x, y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2}$. Für $n = 1$ ist dies $d(x_1, y_1) = |x_1 - y_1|$, also der Abstand von x_1 und y_1 auf der reellen Zahlengeraden, für $n = 2$ und $n = 3$ erhalten wir den Abstand zwischen Punkten in der Ebene bzw. im Raum. Dasselbe gelingt auch in höherer Dimension. Ein bemerkenswerter und grundlegender Satz über die Abstände im $\mathbb{R}^n$ ist der folgende:

Satz A (Dreiecksungleichung): Für je drei Punkte $x, y, z \in \mathbb{R}^n$ gilt $d(x, z) \leq d(x, y) + d(y, z)$. Gleichheit $d(x, z) = d(x, y) + d(y, z)$ gilt genau dann, wenn y auf der Strecke von x nach z liegt.

Beweis: Der Beweis ist etwas knifflig. Sie lernen ihn in der Analysis kennen. In der Regel zeigen Sie zuerst die Cauchy-Schwarzsche Ungleichung und leiten daraus die Dreiecksungleichung ab. □

Was ist ein Quader? Unsere Ecken A und B im Quader können wir als Punkte im $\mathbb{R}^3$ darstellen durch $A = (A_1, A_2, A_3) = (0, 0, 0)$ und $B = (B_1, B_2, B_3) = (100, 45, 60)$. Der ausgefüllte Quader ist dann die Menge $V = \{\, (x_1, x_2, x_3) \in \mathbb{R}^3 \mid A_i \leq x_i \leq B_i \text{ für } i = 1, 2, 3 \,\}$. Die Quaderfläche $Q = \{\, x \in V \mid x_i \in \{A_i, B_i\} \text{ für mind. ein } i = 1, 2, 3 \,\}$ setzt sich aus den sechs Seiten zusammen.

Was ist ein Weg? Wir beobachten eine Ameise, die auf der Quaderfläche Q von A nach B läuft. Zu jeder Zeit $t \in [a, b]$ bezeichnen wir ihre Position mit $\gamma(t) \in Q \subset \mathbb{R}^3$. Wir erhalten so die Abbildung $\gamma\colon [a, b] \to Q\colon t \mapsto \gamma(t)$. Jede Ameise bewegt sich „stetig“, sie kann sich nicht „teleportieren“. Zur Präzisierung benötigen wir daher den Begriff der **stetigen Abbildung**. Die folgende Definition der Stetigkeit kennen Sie vielleicht aus der Schule. Anschaulich stellt man sich gerne vor, dass eine stetige Abbildung „keine Sprünge“ macht und sich „durchgehend zeichnen“ lässt. Das ist eine hilfreiche Umschreibung, aber allzu vage: Wie sollten wir das konkret nachprüfen? Hängt die Stetigkeit von γ etwa vom Betrachter ab, wie genau er Sprünge erkennt oder wie gut er zeichnen kann? Etwas genauer bedeutet Stetigkeit, dass Punkte, die nahe beieinander liegen, auf Punkte abgebildet werden, die ebenfalls nahe beieinander liegen. Auch das ist noch zu vage: Damit kann man nicht rechnen! Um alle Unklarheiten zu beseitigen, werden stetige Abbildungen folgendermassen definiert. Erkennen Sie darin die anschauliche Beschreibung wieder?

Definition 1: Eine Abbildung $f\colon X \to Y$ von $X \subseteq \mathbb{R}^n$ nach $Y \subseteq \mathbb{R}^m$ heißt *stetig*, falls in jedem Punkt $x \in X$ gilt: Für jedes noch so kleine $\varepsilon > 0$ existiert ein geeignetes $\delta > 0$, sodass für jeden Punkt $x' \in X$ mit $d(x, x') < \delta$ der Bildpunkt $f(x')$ einen Abstand $d(f(x), f(x')) < \varepsilon$ hat.

Definition 2: Gegeben sei eine Teilmenge $X \subseteq \mathbb{R}^n$ und zwei Punkte $A, B \in X$. Ein *Weg* von A nach B in X ist eine stetige Abbildung $\gamma\colon [a, b] \to X$ mit $a < b$ sowie $\gamma(a) = A$ und $\gamma(b) = B$.

Die Abbildung γ gibt zu jedem Zeitpunkt $t \in [a, b]$ die Position $\gamma(t) \in X \subseteq \mathbb{R}^n$ an.

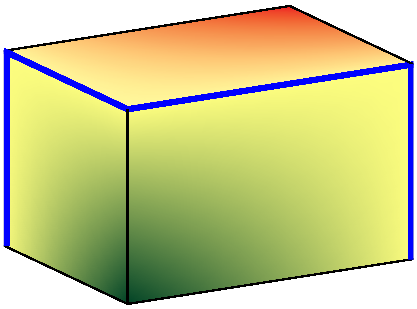
Gerade Wege: Die Abbildung $\sigma\colon [0, T] \to \mathbb{R}^n\colon t \mapsto A + t \cdot (B - A)/T$ ist stetig. Dieser Weg verläuft von $\sigma(0) = A$ nach $\sigma(T) = B$ mit konstantem Geschwindigkeitsvektor $v = (B - A)/T$.

Um unsere erste Behauptung zu zeigen, verwenden wir den folgenden grundlegenden Satz:

Satz B (Zwischenwertsatz): Sei $f\colon [a, b] \to \mathbb{R}$ eine stetige Funktion. Dann nimmt f jeden Wert z zwischen $f(a)$ und $f(b)$ an, das heißt es existiert (mindestens) ein $t \in [a, b]$ mit $f(t) = z$. Insbesondere hat jede stetige Funktion $f\colon [a, b] \to \mathbb{R}$ mit $f(a) \leq 0 \leq f(b)$ eine Nullstelle.

Beweis: Dies beweisen Sie im Mathematikstudium in Ihrer Vorlesung **Analysis 1**. □

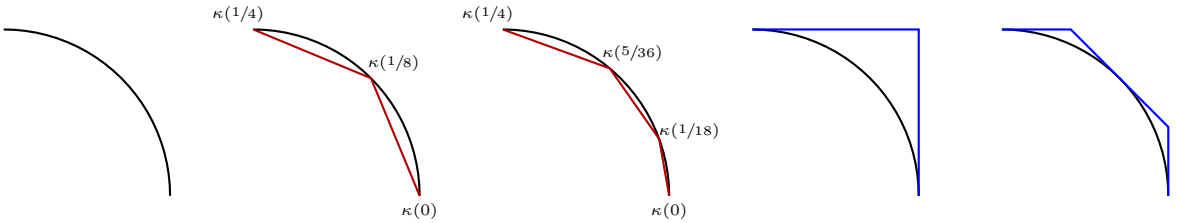
Behauptung 1: Jeder Weg $\gamma\colon [a,b] \to Q$ von A nach B führt über den Äquator, das heißt: Es existiert ein Zeitpunkt $t_0 \in [a,b]$, sodass der Wegpunkt $P = \gamma(t_0)$ auf dem Äquator liegt.



Beweis: Wir wählen eine „Breitengrad-Funktion“ $h\colon Q \to \mathbb{R}$, die stetig ist mit $h(A) < 0$ und $h(B) > 0$, sodass $h(P) = 0$ genau dann gilt, wenn P auf dem Äquator liegt. Solche Abbildungen gibt es, sogar sehr viele. Ein besonders einfaches Beispiel ist gegeben durch $h(x) = (x_1 - B_1)(x_2 - B_2)(x_3 - B_3) + (x_1 - A_1)(x_2 - A_2)(x_3 - A_3)$. Als polynomielle Abbildung ist diese Funktion stetig. Alle geforderten Eigenschaften lassen sich sorgfältig nachprüfen. Die Abbildung rechts illustriert diese Funktion: Grün steht für negative Werte, Rot für positive Werte, reines Gelb für den Wert 0 wird genau auf dem Äquator angenommen. Die Abbildung $f = h \circ \gamma\colon [a,b] \to Q\colon t \mapsto h(\gamma(t))$ ist stetig als Verkettung stetiger Funktionen. Sie gibt an, auf welchem „Breitengrad“ sich der Weg zum Zeitpunkt t befindet. Es gilt $f(a) = h(A) < 0$ und $f(b) = h(B) > 0$. Dank Zwischenwertsatz (Satz B) besitzt f eine Nullstelle $t_0 \in [a,b]$. Der Wegpunkt $P = \gamma(t_0)$ erfüllt $h(P) = f(t_0) = 0$, liegt also auf dem Äquator. □

Bemerkung: Der Beweis per Zwischenwertsatz ist raffiniert und elegant. Müssen Mathematiker:innen es immer so genau nehmen? Ja, das müssen sie! Als mahnendes Beispiel betrachten wir über den rationalen bzw. reellen Zahlen $K = \mathbb{Q}, \mathbb{R}$ die Kreislinie $S = \{\, (x,y) \in K^2 \mid x^2 + y^2 = 1 \,\}$ als Löwenkäfig. Der Löwe sitzt im Ursprung $(0,0)$ und will nach $(1,1)$ ausbrechen. Gibt es eine stetige Abbildung $\gamma\colon \{\, t \in K \mid 0 \le t \le 1 \,\} \to K^2$ von $\gamma(0) = (0,0)$ nach $\gamma(1) = (1,1)$, die S nicht trifft? Für $K = \mathbb{R}$ ist der reelle Löwe gefangen: Dies garantiert der Zwischenwertsatz! Für $K = \mathbb{Q}$ kann der rationale Löwe geradewegs ausbrechen entlang $\gamma(t) = (t,t)$. Wer hätte das gedacht?

Wie messen wir die Länge eines Weges? Wir betrachten zuerst ein Beispiel, nämlich den Weg $\kappa\colon [0, 1/4] \to \mathbb{R}^2\colon t \mapsto (\cos(2\pi t), \sin(2\pi t))$ entlang eines Viertelkreises. Um die Länge zu messen, unterteilen wir das Intervall $[0, 1/4]$ an beliebigen Stellen $0 = t_0 < t_1 < t_2 < \ldots < t_{n-1} < t_n = 1/4$.



Die Punkte $\kappa(t_0), \kappa(t_1), \kappa(t_2), \ldots, \kappa(t_{n-1}), \kappa(t_n)$ definieren einen Polygonzug der Länge

$$\ell(\kappa; t_0, t_1, \ldots, t_n) = d(\kappa(t_0), \kappa(t_1)) + d(\kappa(t_1), \kappa(t_2)) + \cdots + d(\kappa(t_{n-1}), \kappa(t_n))$$

kurz $\sum_{i=1}^{n} d(\kappa(t_{i-1}), \kappa(t_i))$. Die roten Linien in der zweiten und dritten Graphik sind solche Polygonzüge, der erste hat die Länge $2\sqrt{2-\sqrt{2}} \approx 1.5307$, der zweite ist etwas länger. Egal welche Unterteilung wir wählen, der blaue Polygonzug in der vierten Grafik ist länger: Dies sieht man durch geschickte mehrfache Anwendung der Dreiecksungleichung (Übung). Die Länge 2 des blauen Polygonzugs ist also eine obere Schranke für alle $\ell(\kappa; t_0, t_1, \ldots, t_n)$. Auch die Länge des blauen Polygonzugs $2 \cdot (\sqrt{2} - 1) + 2 \cdot \sqrt{3 - 2\sqrt{2}} \approx 1.6569$ in der fünften Grafik ist eine obere Schranke. Es gibt noch kleinere obere Schranken. Die Länge des Weges κ ist die kleinste all dieser oberen Schranken, genannt das *Supremum*, geschrieben $\sup$. Dies machen wir zur allgemeinen Definition:

Definition 3: Sei $\gamma\colon [a,b] \to X \subseteq \mathbb{R}^m$ ein Weg. Die *Länge* von γ definieren wir durch

$$\ell(\gamma) = \sup\big\{\, \ell(\gamma; t_0, t_1, \ldots, t_n) \;\big|\; a = t_0 < t_1 < \ldots < t_n = b \,\big\}.$$

Wir nutzen hier eine besondere Eigenschaft: Die reellen Zahlen $\mathbb{R}$ sind vollständig! Jede Menge $M \subseteq \mathbb{R}$, die nicht-leer und nach oben beschränkt ist, besitzt in $\mathbb{R}$ eine kleinste obere Schranke, geschrieben $\sup M$. (In $\mathbb{Q}$ gilt das nicht!) Ist M nach oben unbeschränkt, so setzen wir $\sup M = \infty$.

Beispiel: Für $\kappa\colon [0, 1/4] \to \mathbb{R}^2\colon t \mapsto (\cos(2\pi t), \sin(2\pi t))$ ist die Länge $\ell(\kappa)$ größer als 1.53, denn jede obere Schranke ist mindestens so groß wie die Länge des roten Polygonzugs in der zweiten Graphik. Andererseits ist die Länge $\ell(\kappa)$ höchstens 1.657, denn diese obere Schranke entnehmen wir der fünften Graphik. Diese Eingrenzungen lassen sich durch feinere Polygonzüge beliebig verbessern. Als kleinste obere Schranke findet man schließlich $\ell(\kappa) = \pi/2 \approx 1.5708$.

Beispiel: Die Länge des Weges $\sigma\colon [0,1] \to \mathbb{R}^n\colon t \mapsto A + t \cdot (B - A)$ ist $\ell(\sigma) = d(A, B)$. Dies folgt mit Hilfe der Dreiecksungleichung (Satz A). Das ist nicht überraschend, sondern beruhigend.

Behauptung 2: Jeder kürzeste Weg $\gamma\colon [a, b] \to \mathbb{R}^n$ von A nach B hat die Länge $d(A, B)$ und verläuft entlang der Verbindungsstrecke. (Genauer ist γ eine monotone Umparametrisierung von σ.)

Beweis: Der Weg σ hat die Länge $d(A, B)$. Für γ betrachten wir die Unterteilung $a = t_0 < t_1 = b$ und finden $d(A, B) = \ell(\gamma; t_0, t_1) \leq \ell(\gamma)$. Somit ist $d(A, B)$ die kürzest mögliche Länge für einen Weg von A nach B. Angenommen, es gibt einen Zeitpunkt $t_1 \in [a, b]$, für den $\gamma(t_1)$ außerhalb der Strecke von A nach B liegt. Dann ist $d(A, B) < d(A, \gamma(t_1)) + d(\gamma(t_1), B) = \ell(\gamma; a, t_1, b) \leq \ell(\gamma)$. Die erste Ungleichung gilt wegen der Dreiecksungleichung und ist strikt (Satz A). Somit ist γ echt länger als die direkte Verbindung σ. (Mit ähnlichen Argumenten konstruiert man die Umparametrisierung von σ zu $\gamma = \sigma \circ u$ mit $u\colon [a, b] \to [0, 1]$ monoton und stetig.) □

Demnach verläuft jeder kürzeste Weg γ von A nach B für eine fliegende Ameise entlang der Strecke zwischen A und B und hat die Länge $\ell(\gamma) = d(A, B) = \sqrt{p^2 + q^2 + r^2}$.

Behauptung 3: Für jeden kürzesten Weg $\gamma\colon [a, b] \to Q$ von A nach B auf der Quaderfläche gilt: Es gibt einen Punkt $P = \gamma(t_0)$ auf dem Äquator, sodass der Teilweg $\gamma_1\colon [a, t_0] \to Q$ auf der Strecke von A nach P verläuft und der Teilweg $\gamma_2\colon [t_0, b] \to Q$ auf der Strecke von P nach B.

Beweis: Nach Behauptung 1 finden wir ein $t_0 \in [a, b]$, sodass $P = \gamma(t_0)$ auf dem Äquator liegt. Der Teilweg $\gamma_1\colon [a, t_0] \to Q$ muss ein kürzester Weg von A nach P in Q sein, ansonsten ließe sich auch γ abkürzen. Jeder kürzeste Weg von A nach P in $\mathbb{R}^3$ verläuft entlang der Strecke zwischen A und P. Da diese Strecke in der Quaderfläche Q enthalten ist, ist dieser auch ein kürzester Weg von A nach P in Q. Somit verläuft γ_1 entlang der Strecke zwischen A und P. Dasselbe gilt für den zweiten Teilweg γ_2 von P nach B. □

Demnach gilt $\ell(\gamma) = d(A, P) + d(P, B)$, wir müssen also nur noch P auf dem Äquator variieren. Das ist ein relativ einfaches, eindimensionales Optimierungsproblem und wurde in Stufe 1 bereits gelöst: Wir haben sechs mögliche Übergangspunkte P auf dem Äquator identifiziert, und jeder kürzeste Weg verläuft über einen dieser Punkte. So finden wir schießlich *alle* kürzesten Wege.

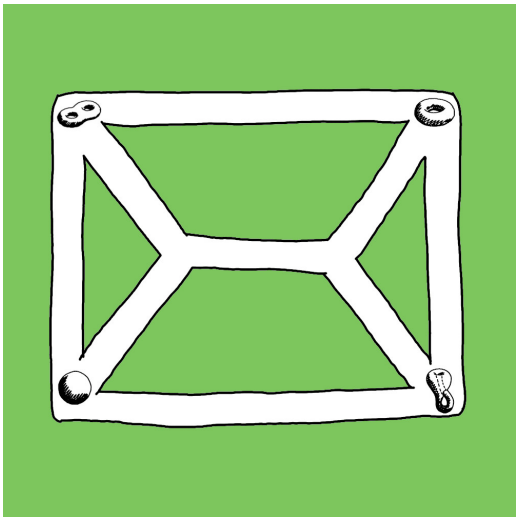
Wie zählen wir Wege? Wir wollen schließlich zählen, wie viele kürzeste Wege es von A nach B in Q gibt. Dabei stoßen wir auf ein Problem: Nach obiger Definition gibt es unendlich viele! Wir können jeden Weg in verschiedenen Geschwindigkeiten durchlaufen, also monoton umparametrisieren, ohne seine Weglänge zu verändern. Wir wollen daher Wege zusammenfassen, die sich nur in der Geschwindigkeit unterscheiden. Die eleganteste Möglichkeit ist, dass wir nur Wege $\gamma\colon [0, 1] \to Q$ mit einer konstanten Geschwindigkeit c betrachten: Für jeden Zeitpunkt $t \in [0, 1]$ hat der Teilweg $\gamma|_{[0,t]}\colon [0, t] \to Q$ bis zur Zeit t die Länge $\ell(\gamma|_{[0,t]}) = ct$. In diesem Sinne gilt: Auf der Quaderfläche Q gibt es von A nach B genau zwei kürzeste Wege mit konstanter Geschwindigkeit.

Ein Weg $\gamma\colon [0, 1] \to X \subseteq \mathbb{R}^n$ mit konstanter Geschwindigkeit heißt **Geodäte**, falls er lokal ein kürzester Weg ist. Das bedeutet: Zu jedem Zeitpunkt $t \in [0, 1]$ existiert $\varepsilon > 0$ sodass $\gamma|_I$ auf dem Intervall $I = [t_0, t_1] = [t - \varepsilon, t + \varepsilon] \cap [0, 1]$ ein kürzester Weg von $\gamma(t_0)$ nach $\gamma(t_1)$ in X ist. Alle Beispielwege aus Stufe 1, die sich $n + 1/2$ mal um den Quader wickeln, erfüllen dies!

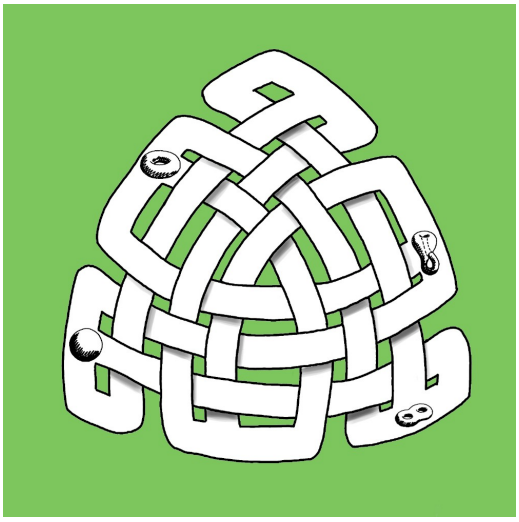
Universität Stuttgart

Beispielaufgabe zur Studienwahl

Mathematische Schatzsuche: der Blick für das Wesentliche



Labyrinth 1



Labyrinth 2

Sammeln Sie in beiden Labyrinthen alle vier mathematischen Schätze! Laufen Sie dazu einen geschlossenen Weg, das heißt hören Sie dort auf, wo Sie angefangen haben. An jeder Stelle dürfen Sie höchstens einmal vorbeikommen, außer natürlich am Anfangs- und Endpunkt.

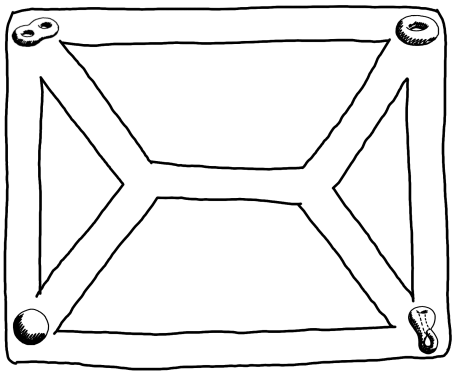
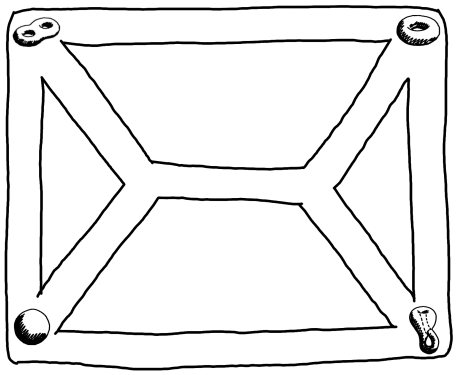
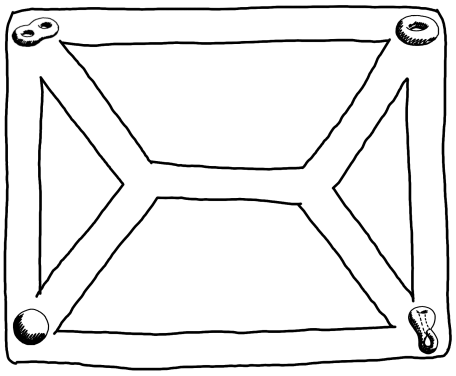
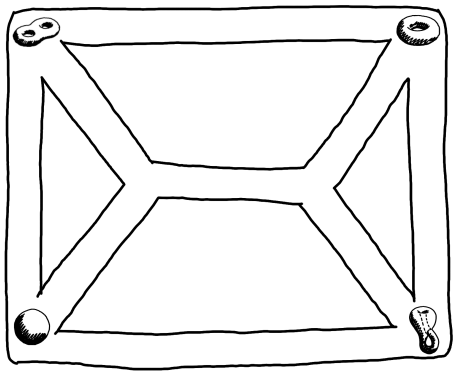
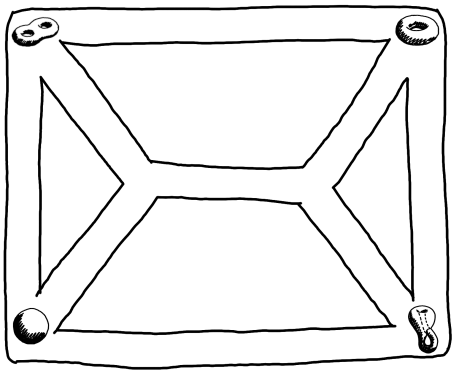
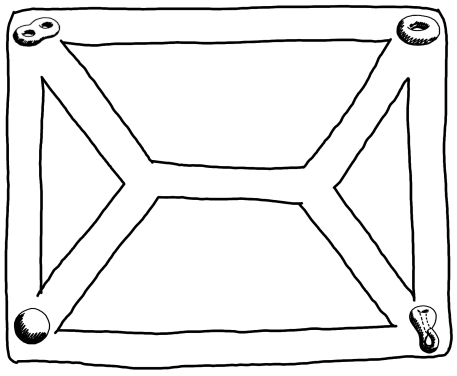
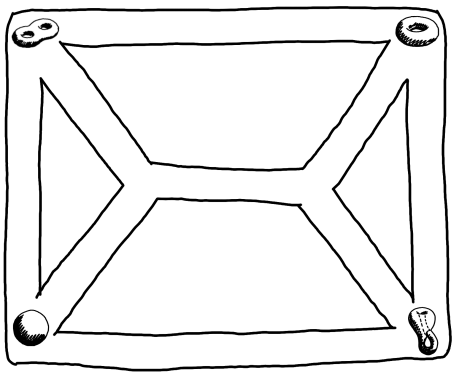
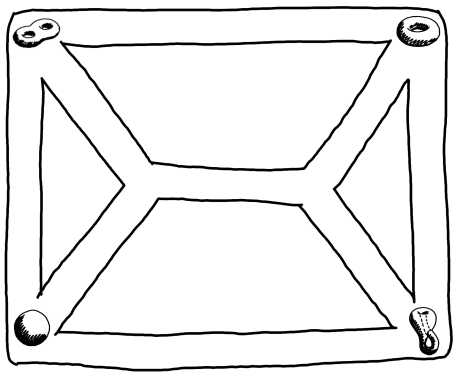
Welche der folgenden Informationen benötigen Sie tatsächlich, um solch ein Rätsel lösen zu können?

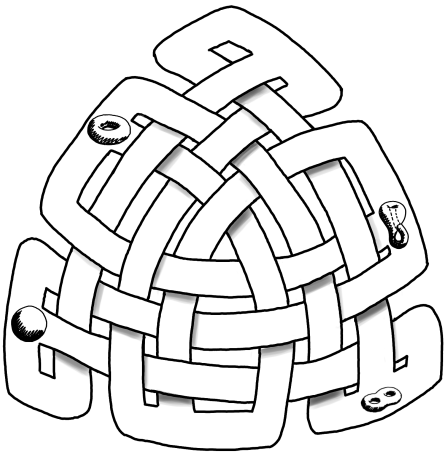
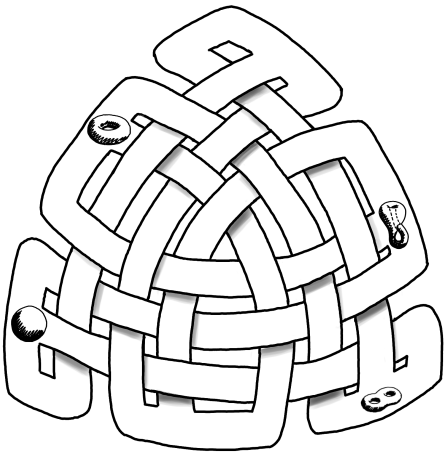
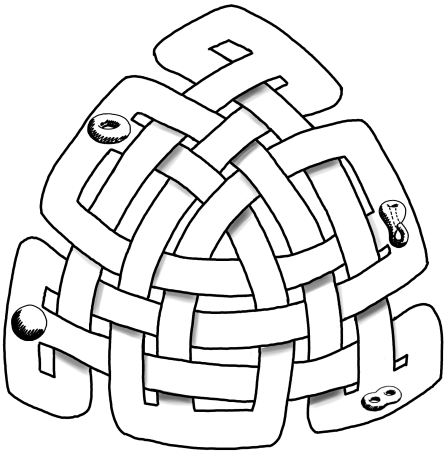
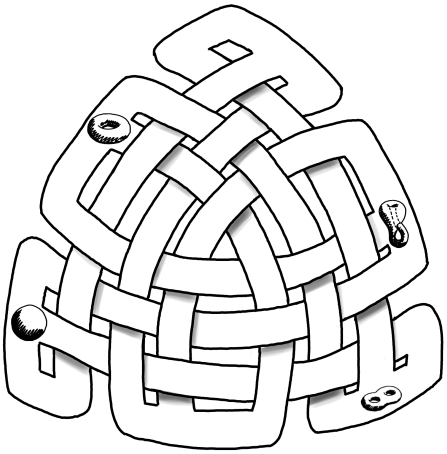
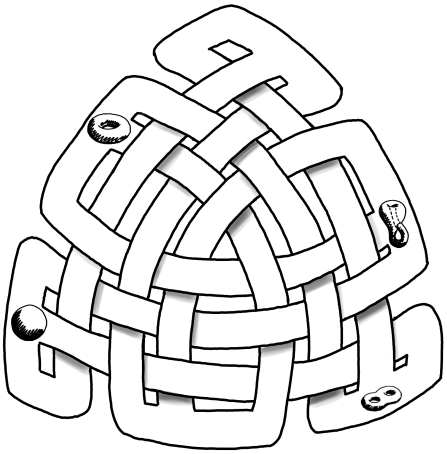
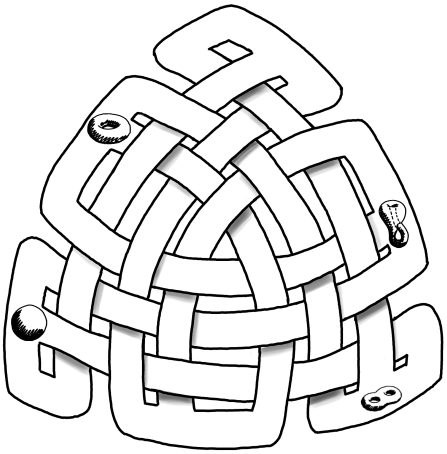
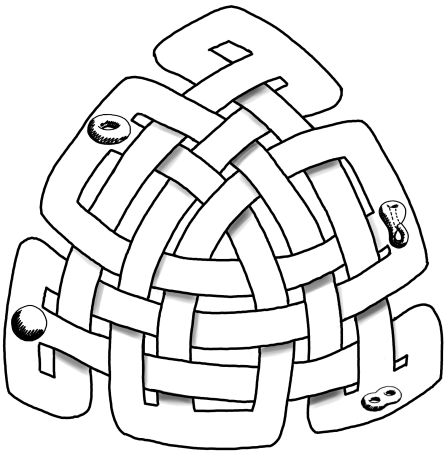
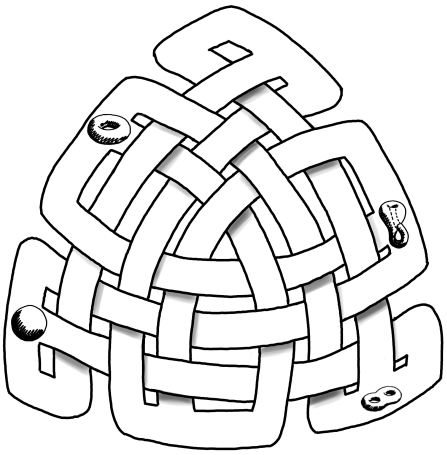
	ja	nein
• die Menge der Weggabelungen, an denen drei oder mehr Wegstücke zusammentreffen	☐	☐
• die genaue Position der Gabelungen in Koordinaten	☐	☐
• die Menge der Über- und Unterkreuzungen	☐	☐
• welche Gabelungen durch direkte Wegstücke verbunden sind	☐	☐
• die Länge der einzelnen Wegstücke	☐	☐

Wie viele Lösungen gibt es? Zählen Sie alle Lösungswege! Dabei sollen zwei Wege nur einmal gezählt werden, wenn sie sich nur durch die Durchlaufungsrichtung unterscheiden; ebenso soll die Position des Anfangspunkts keine Rolle spielen.

	keine	1	2	3	4	5	6	7	8	9	mind. 10	∞	
Für Labyrinth 1 gibt es	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Lösungen.
Für Labyrinth 2 gibt es	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Lösungen.

mathematik fakultät8

Stufe 0 / Kurzantwort: Für die Problemlösung spielt es tatsächlich keine Rolle, wo genau die Weggabelungen liegen, wo die Wege verlaufen oder wie lang sie sind. Genauso unwichtig ist es, ob sich Wege über- / unterkreuzen oder nicht. Um unser Problem zu lösen, müssen wir nur wissen, an welchen Gabelungen sich welche Wegstücke treffen, und natürlich an welchen Positionen die Schätze liegen. Eine solche Struktur bestehend aus Knoten (hier Gabelungen) und Kanten (Wegstücke zwischen zwei Gabelungen) nennt man in Mathematik und Informatik einen *Graphen*.

- **Labyrinth 1:** Hier gibt es genau sechs Lösungen. Diese finden Sie mit Geduld und Geschick; so sehen Sie, dass es *mindestens* sechs Lösungen gibt. Wie können Sie sicher sein, dass es keine weitere Lösung gibt? Nur durch Sorgfalt, damit Ihnen kein Fall entgeht.
- **Labyrinth 2:** Das zweite Labyrinth sieht auf den ersten Blick viel komplizierter aus als das erste. Aber das täuscht: Für die vorliegende Fragestellung sind beide gleich! Daher gibt es auch hier sechs Lösungen. Abstraktion strukturiert und vereinfacht!

Stufe 1 / Ausführung: *Hier erfahren Sie, wie Sie konkret vorgehen, um* alle *Lösungen zu finden.*

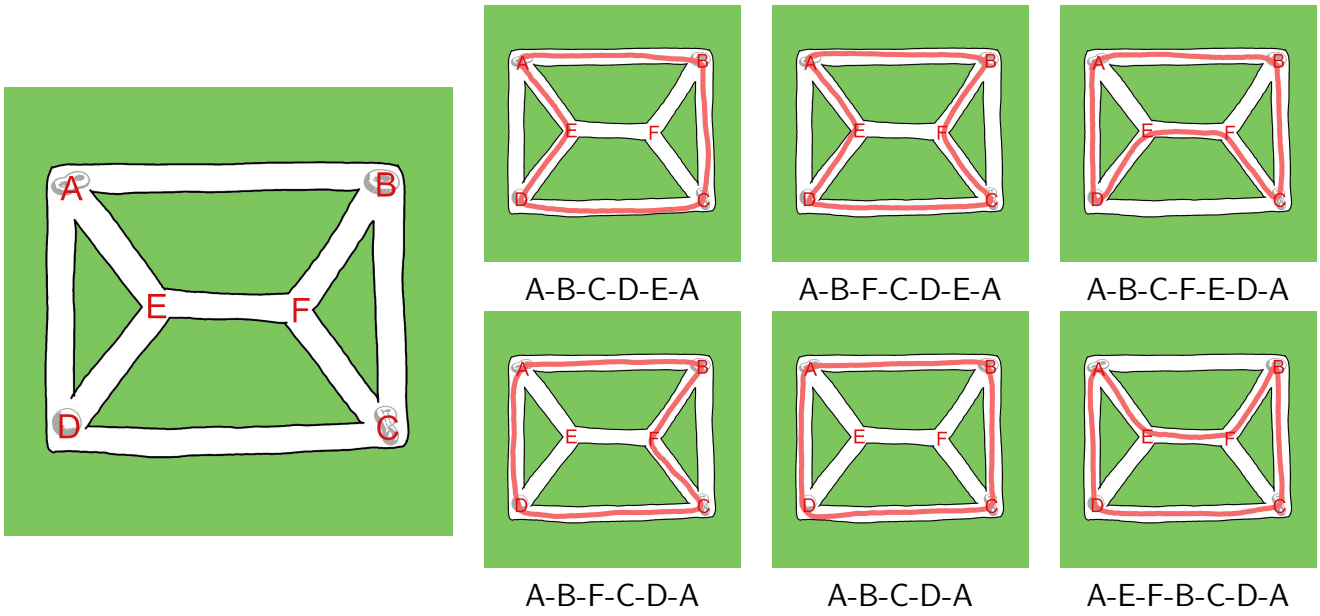


Abbildung 1: Labyrinth 1 und die sechs Lösungen

Bilder sind schön und nützlich, aber leider auch aufwändig. Um nicht immer Bilder zeichnen zu *müssen*, nutzen wir eine kurze und bequeme Notation. Hierzu beschriften wir die Gabelungen in **Labyrinth 1** mit den Buchstaben A, B, C, D, E, F wie in Abbildung 1. Das Labyrinth lässt sich dann kurz und einfach beschreiben durch die folgenden Angaben:

- Die Gabelungen A, B, C, D, E, F.
- Die Wegstücke AB, AD, AE, BC, BF, CD, CF, DE, EF.
- Die Positionen der vier mathematischen Schätze A, B, C, D.

Die folgenden Überlegungen können Sie anhand der Bilder nachvollziehen, alternativ erlaubt unsere Kurznotation auch ohne Bild zu arbeiten. In dieser Form kann das Labyrinth insbesondere einem Computer übergeben werden, der – richtig programmiert – alle Möglichkeiten absucht. Das vorliegende Problem ist glücklicherweise klein genug, sodass wir es von Hand lösen können.

Behauptung: Labyrinth 1 besitzt genau die sechs Lösungen aus Abbildung 1.

Das beinhaltet drei Teilfragen: (1) Wie überprüfen wir vorgelegte Lösungen? Die Regeln sind hier leicht nachzuprüfen – auch anhand der abstrakten Daten. (2) Wie finden wir möglichst viele Lösungen? (3) Wie garantieren wir, dass wir alle Lösungen gefunden haben?

Beweis der Behauptung: Ein Lösungsweg muss an Position A vorbeikommen, daher muss er genau zwei der drei Wegstücke AB, AE und AD nutzen. Wir unterscheiden drei Fälle:

- Die Lösung durchläuft AB und AE, aber nicht AD: Da der Weg auch an Position D vorbeiführen muss, sind die Wegstücke DE und CD Teil des Weges. Dann kann aber EF nicht Teil des Weges sein. Es gibt daher zwei solche Lösungen: **A-B-C-D-E-A** und **A-B-F-C-D-E-A**.
  Wir haben hier die Gabelungen der Reihe nach aufgelistet, in der sie durchlaufen werden. Doch Achtung! Diese Darstellung ist nicht eindeutig: Zum Beispiel bezeichnen A-B-C-D-E-A, A-E-D-C-B-A (rückwärts durchlaufen) und B-C-D-E-A-B (anderer Startpunkt) dieselbe Lösung.
- Die Lösung durchläuft AB und AD, aber nicht AE: Führt der Weg über E, dann auch über F, wir erhalten die Lösung **A-B-C-F-E-D-A**. Führt der Weg nicht über E, dann gibt es die zwei Lösungen **A-B-F-C-D-A** und **A-B-C-D-A**.
- Die Lösung durchläuft AD und AE, aber nicht AB: Dann kann DE nicht Teil des Weges sein, denn sonst wäre der Weg schon geschlossen. Daher ist EF Teil des Weges, ebenso BF und BC. Hier finden wir also eine Lösung **A-E-F-B-C-D-A**.

Sie können die abstrakte Notation als Wegbeschreibung nutzen und so in das Bild zurückübersetzen.

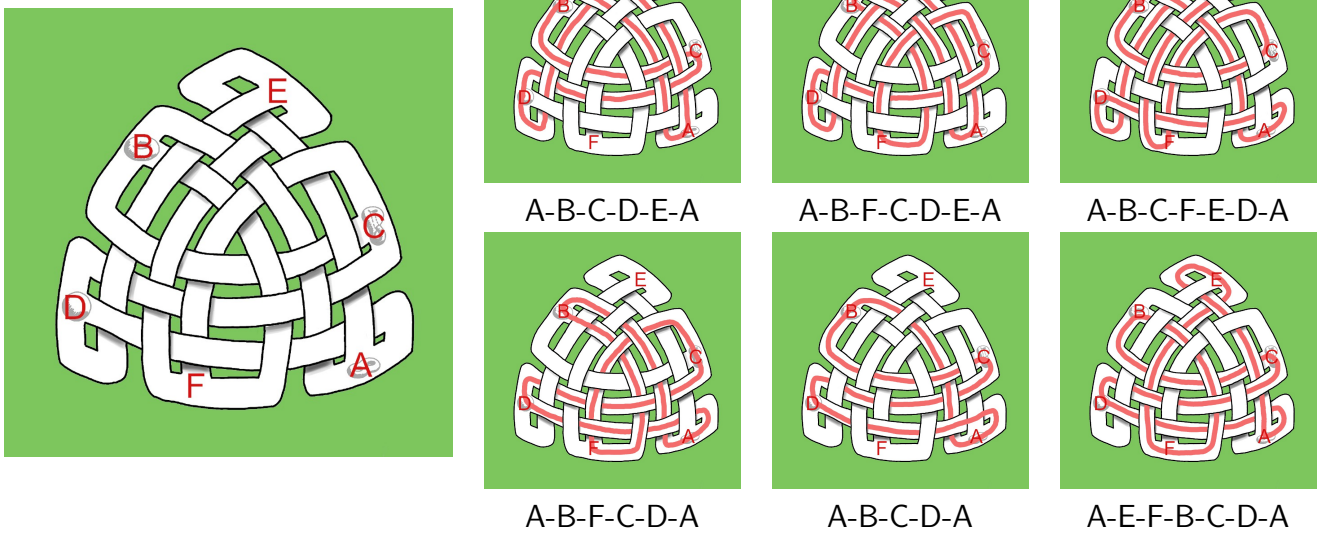


Abbildung 2: Labyrinth 2 und die sechs Lösungen

Auch das **Labyrinth 2** können wir kurz und präzise wie folgt beschreiben:

- Die Gabelungen A, B, C, D, E, F.
- Die Wegstücke AB, AD, AE, BC, BF, CD, CF, DE, EF.
- Die Positionen der vier mathematischen Schätze A, B, C, D.

Fällt Ihnen etwas auf? Ja, richtig! Die hier extrahierten wesentlichen Daten sind genau dieselben wie bei Labyrinth 1! Daher sind auch die (abstrakten) Lösungen dieselben. Die Buchstaben haben wir dabei nicht zufällig gewählt, sondern geschickt so, dass Sie die Analogie sofort sehen.

Stufe 2 / Was will und soll diese Aufgabe?

Nach der Lösung dieser Aufgabe erläutern wir als Rück- und Ausblick, warum wir diese Problemstellung mathematisch interessant finden und inwiefern sie repräsentativ ist für das Mathematikstudium.

Bei unserer Untersuchung nutzen wir verschiedene mathematische Methoden. Um Labyrinth 1 zu lösen, gehen wir systematisch alle Fälle durch; in der Mathematik nennt man das *Fallunterscheidung*. Hierzu sind vor allem Sorgfalt, Konzentration und Buchführung gefragt, damit wir keinen Fall übersehen oder vergessen. Dabei hilft uns insbesondere eine effiziente, sachgerechte *Notation*. Sie dient zur Dokumentation für den Autor und zur Kommunikation mit anderen.

By relieving the brain of all unnecessary work, a good notation
sets it free to concentrate on more advanced problems.
(Alfred North Whitehead, 1861–1947, *An Introduction to Mathematics*, 1911)

Das Sorgfaltsprinzip gilt allgemein, insbesondere in der Mathematik: Ein Beweis kann in noch so vielen Schritten richtig sein; wenn uns an einer einzigen Stelle ein Fehler unterläuft, dann ist der Beweis nicht vollständig, und die Behauptung weiterhin unbewiesen, vielleicht sogar falsch.

Die Lösungen zu Labyrinth 2 haben wir ohne jede Mühe geschenkt bekommen. *Solve one, get one free!* Warum ist das so leicht? Wir nutzen eine typisch mathematische Vorgehensweise: Anstatt das Rad immer wieder neu zu erfinden, führen wir ein neues Problem auf ein altes, bereits gelöstes zurück. Das Zauberwort heißt *Abstraktion*: Wenn Sie den Kern eines Problems oder einer Methode erst einmal erkannt haben, dann können Sie dies immer wieder anwenden – auch auf neue Probleme, die zunächst sehr verschieden aussehen. Effiziente mathematische Arbeit beruht auf genau dieser Fähigkeit: Sie sollen treffsicher erkennen, dass das Problem eigentlich schon gelöst wurde.

Sie können Labyrinth 2 sicherlich auch durch Ausprobieren lösen, aber vermutlich werden Sie schnell durcheinander kommen, da die verschlungenen Wege nicht so einfach zu erfassen sind. Abstraktion ist die Kunst, das Wesentliche zu erkennen und vom Unwesentlichen zu trennen!

Allgemein stehen Mathematiker:innen sowohl im Studium als auch im Beruf oft vor einem gegebenen Problem, zu dem sie alle Lösungen finden wollen oder müssen. Das Vorgehen ähnelt meist unserem Beispiel. Abstraktion hilft, sie strukturiert und vereinfacht: Was sind die relevanten Daten? Wie prüft man eine Lösung? Wie findet man möglichst viele Lösungen? Wie kann man garantieren, alle Lösungen gefunden zu haben?

Einordnung in das Mathematikstudium. Die **Graphentheorie** ist ein eigenes Gebiet der Mathematik, das sowohl praktisch wichtig als auch theoretisch interessant ist. Es wird auch in der Informatik intensiv genutzt, als universeller Datentyp zum Beispiel bei der Routenplanung. Das berühmteste Beispiel ist das *Problem des Handlungsreisenden*.

Wir können uns dazu Varianten unseres Labyrinths vorstellen, beispielsweise zu besuchende Orte und mögliche Verbindungen. Wenn wir den kürzesten bzw. günstigsten Lösungsweg suchen, dann benötigen wir für die Problemlösung zusätzliche Daten, etwa die Längen der einzelnen Wegstücke oder die Kosten jeder Strecke. Das sind überaus praxisnahe Probleme, deren Lösung Sie täglich dankend nutzen, zum Beispiel, wenn Sie ein Navigationsgerät verwenden oder ein Bahnticket kaufen.

Als Mathematiker:in sind Sie nicht nur Konsument, sondern auch Produzent solcher optimierten Lösungen und sorgfältigen Begründungen, Sie nutzen und erschaffen Sätze und Beweise, Algorithmen und Programme. Die hierzu nötigen Techniken erlernen Sie im Mathematikstudium, angefangen bei den theoretischen Grundlagen über typische Anwendungen bis hin zur Programmierung.

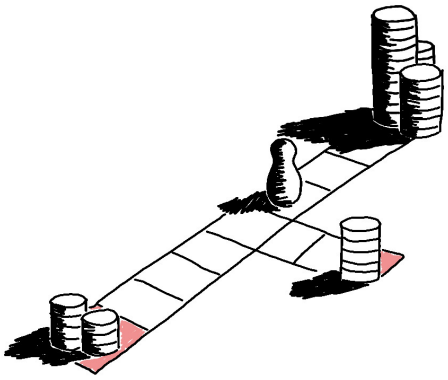
Universität Stuttgart

Beispielaufgabe zur Studienwahl

Mathematische Prognose: Welcher Gewinn erwartet Sie?

Sie setzen Ihren Spielstein auf ein Feld eines Spielbretts, wie im Bild rechts. In jedem Zug würfeln Sie aus, auf welches Nachbarfeld Sie weiterziehen, auf jedes mit gleicher Wahrscheinlichkeit. Das Spiel endet am Rand in einem roten Feld mit dem angegebenen Gewinn. Welchen Gewinn erwarten Sie jeweils bei Start in einem weißen Feld?

Hinweis: Sie können sich überlegen und dann nutzen, dass jeder Erwartungswert auf einem weißen Feld der Mittelwert seiner Nachbarn ist.



Zwei einfache Beispiele:

Zu | 2 | | 14 | sind die erwarteten Gewinne | 2 | 8 | 14 |.

Zu | 2 | | | 14 | sind die erwarteten Gewinne | 2 | 6 | 10 | 14 |.

Spiel 1: Welchen Gewinn erwarten Sie auf jedem weißen Feld?

7								23

Spiel 2: Dieselbe Frage für das folgende interessantere Spielbrett. Das zentrale Feld hat nun drei gleichwahrscheinliche Nachbarn.

7								23
				5				

mathematik fakultät8

Stufe 0 / Kurzantwort: In jedem roten Feld z ist der Gewinn $u(z)$ vorgegeben. Sie suchen für jedes weiße Feld z seinen Erwartungswert $u(z)$. Dieser soll der Mittelwert seiner Nachbarn sein! Warum? Im nächsten Zug gehen Sie mit gleicher Wahrscheinlichkeit auf eines der n Nachbarfelder $z_1, z_2, \ldots, z_n$. Somit ist der erwartete Gewinn auf Ihrem aktuellen Feld $u(z) = \frac{1}{n}[u(z_1) + u(z_2) + \cdots + u(z_n)]$.

Um die Lösungen für die beiden Spielbretter zu finden, gibt es mehrere Möglichkeiten:

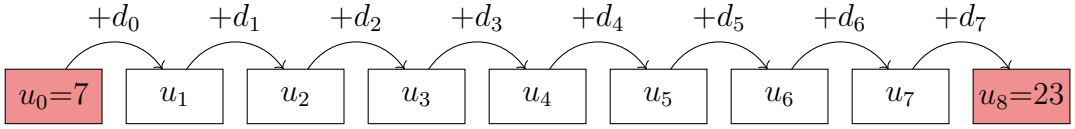
- Durch (gezieltes) Ausprobieren und anschließendes Prüfen. Das funktioniert hier gerade noch, wird aber schwieriger, je komplizierter und größer das Spielbrett und die Auszahlungen werden.
- Durch Ausrechnen der exakten Lösung. Hierzu erstellen Sie ein lineares Gleichungssystem und lösen es mit dem Gauß–Algorithmus aus der Schule. Für kleine Systeme gelingt dies per Hand.
- Durch Näherungsverfahren. Raffinierte numerische Verfahren lohnen sich für große Systeme; die Näherungslösungen sind zwar nicht ganz exakt, dafür aber schnell zu berechnen.

Übrigens gibt es zu jedem der beiden Spiele genau eine Lösung. Anschaulich mag das aus der Aufgabenstellung plausibel erscheinen, dahinter verbirgt sich ein interessanter mathematischer Satz.

Stufe 1 / Ausführung: Zunächst zu **Spiel 1**. Die / eine Lösung ist gegeben durch:

7	9	11	13	15	17	19	21	23

Wenn Sie einen solchen Lösungskandidaten erst einmal (geraten / beschafft / berechnet) haben, dann ist die geforderte Mittelwerteigenschaft leicht nachzuprüfen. Hier gilt sie jedenfalls. Das erklärt noch nicht, wie Sie eine Lösung überhaupt erst finden, und warum es keine weiteren Lösungen gibt. Das erklären wir nun ausführlicher. Die gesuchten Erwartungswerte bezeichnen wir mit $u_1, u_2, \ldots, u_7$:

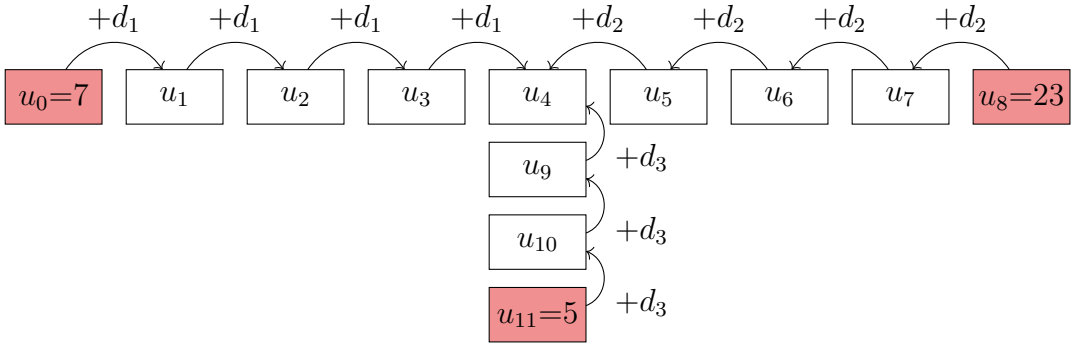


Das Feld 1 erfüllt die Mittelwerteigenschaft $u_1 = \frac{1}{2}(u_0 + u_2)$, also $2u_1 - u_2 = 7$. Genauso stellen wir die Gleichung zu jedem Feld $2, 3, \ldots, 7$ auf und erhalten so das lineare Gleichungssystem

$$\begin{array}{rrrrrrrrr}
2u_1 & -u_2 & & & & & & = & 7 \\
-u_1 & +2u_2 & -u_3 & & & & & = & 0 \\
 & -u_2 & +2u_3 & -u_4 & & & & = & 0 \\
 & & -u_3 & +2u_4 & -u_5 & & & = & 0 \\
 & & & -u_4 & +2u_5 & -u_6 & & = & 0 \\
 & & & & -u_5 & +2u_6 & -u_7 & = & 0 \\
 & & & & & -u_6 & +2u_7 & = & 23
\end{array}$$

Dieses System lässt sich mit etwas Mühe von Hand lösen. Wesentlich einfacher gelingt dies, wenn wir nicht die Erwartungswerte u_i betrachten, sondern die Differenzen $d_0 = u_1 - u_0$, $d_1 = u_2 - u_1$, …, $d_7 = u_8 - u_7$. Diese erfüllen $d_0 + d_1 + \cdots + d_7 = 23 - 7 = 16$. Für jedes Feld $i = 1, 2, \ldots, 7$ bedeutet die Mittelwerteigenschaft $u_i = \frac{1}{2}(u_{i-1} + u_{i+1})$ nun $u_i = \frac{1}{2}(u_i - d_{i-1} + u_i + d_i)$, also $d_i = d_{i-1}$. Alle d_i sind demnach gleich und in der Summe gilt $16 = d_0 + d_1 + \cdots + d_7 = 8d_0$. Folglich ist die eindeutige Lösung $d_0 = d_1 = \cdots = d_7 = 2$. So finden wir (durch Rechnung, nicht durch Raten) die oben vorgeschlagene Lösung und können außerdem garantieren, dass es keine weitere Lösung gibt. Mathematiker:innen sprechen in diesem Fall von Existenz und Eindeutigkeit der Lösung.

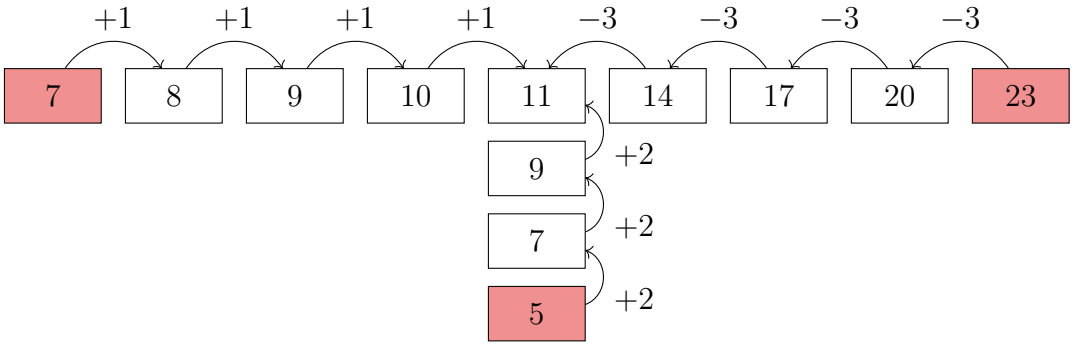
Nun zu **Spiel 2**. Mit demselben Trick lässt sich auch das zweite Spielbrett effizient lösen! Wir überlegen uns zuerst wie in Spiel 1, dass in jedem der drei Arme die Differenzen gleich bleiben:



Es gilt dann $7+4d_1 = 23+4d_2 = 5+3d_3$, denn dies ist der Erwartungswert im mittleren Feld 4. Die Mittelwerteigenschaft für dieses Feld besagt außerdem $d_1 + d_2 + d_3 = 0$. Dies führt zu folgendem linearen Gleichungssystem mit drei Gleichungen in drei Unbekannten:

$$\begin{array}{rrrcr} 4d_1 & -4d_2 & & = & 16 \\ 4d_1 & & -3d_3 & = & -2 \\ d_1 & +d_2 & +d_3 & = & 0 \end{array}$$

Sie finden die eindeutige Lösung $d_1 = 1$, $d_2 = -3$, $d_3 = 2$. (Probe!) Die Lösung ist somit:



Als dritte Lösungsidee raten Sie eine beliebige Näherungslösung; diese wird noch nicht exakt richtig sein, aber Sie können den Fehler schrittweise korrigieren. Am einfachsten gelingt dies mit einer Tabellenkalkuklation, die Sie auf der Seite mit den Beispielaufgaben herunterladen können. Sie können diese mit *LibreOffice* öffnen und selbst experimentieren: Für $t = 0$ geben Sie beliebige Startwerte vor und der Computer berechnet schrittweise die Mittelwerte, zum Beispiel:

Zeit	0	1	2	3	4	5	6	7	8	9	10	11
0	7.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	23.00	0.00	0.00	5.00
1	7.00	3.50	0.00	0.00	0.00	0.00	0.00	11.50	23.00	0.00	2.50	5.00
2	7.00	3.50	1.75	0.00	0.00	0.00	5.75	11.50	23.00	1.25	2.50	5.00
3	7.00	4.38	1.75	0.88	0.42	2.88	5.75	14.38	23.00	1.25	3.13	5.00
4	7.00	4.38	2.63	1.08	1.67	3.08	8.63	14.38	23.00	1.77	3.13	5.00
10	7.00	5.71	5.04	4.58	5.67	8.33	12.79	17.46	23.00	4.53	4.70	5.00
11	7.00	6.02	5.15	5.35	5.82	9.23	12.90	17.89	23.00	5.18	4.77	5.00
12	7.00	6.07	5.69	5.48	6.59	9.36	13.56	17.95	23.00	5.29	5.09	5.00
83	7.00	8.00	9.00	9.99	10.99	13.99	17.00	20.00	23.00	9.00	7.00	5.00
84	7.00	8.00	9.00	10.00	11.00	14.00	17.00	20.00	23.00	9.00	7.00	5.00

Sie sehen ein erstaunliches Phänomen: Die Werte stabilisieren sich für große t. Mathematiker:innen sprechen von *Konvergenz* gegen einen Grenzwert. Dieser Grenzwert ist die gesuchte (exakte) Lösung!

Stufe 2 / Was will und soll diese Aufgabe?

Nach der Lösung dieser Aufgabe erläutern wir als Rück- und Ausblick, warum wir diese Problemstellung mathematisch interessant finden und inwiefern sie repräsentativ ist für das Mathematikstudium.

Prüfen vs Finden. An unseren beiden Beispielen erkennen Sie zunächst folgendes Grundprinzip:

- Es ist oft leicht, für eine vorgelegte Lösung die *Probe* zu machen.
- Es ist meist schwerer, selbst (eine oder alle) Lösungen zu *finden*.

Das ist eine grundsätzliche Asymmetrie: Nach mühsamer Rechnung lohnt sich die leichte Probe; das geht rasch und enttarnt Rechenfehler. Wenn Sie diesen Trick nutzen, arbeiten Sie treffsicherer und effizienter. Auch in der Programmierung sind Proben durch *test cases* nützlich. Ähnlich ist es bei einem mathematischen Satz leichter, einen Beweis nachzuvollziehen, als selbst einen zu entwickeln. Im Mathematikstudium lernen Sie beide Seiten: sorgfältiges Prüfen und kreatives Entwickeln.

Viele Anwendungen, gemeinsame Struktur. Unsere Beispielaufgaben und ihre Lösungsmethoden sind nicht nur für Spiele interessant, sondern treten in überraschend vielfältigen Anwendungen auf:

- Hooke: Ein I- oder Y-förmiges Netz aus ideal leichten Federn wird am Rand auf verschiedenen Höhen fixiert. Auf welche Ruhelage pendelt es sich ein? Wir finden dieselben Gleichungen!
- Kirchhoff: An eine I- oder Y-förmige Schaltung aus gleichen Widerständen werden am Rand feste elektrische Spannungen angelegt. Welche Spannungen messen Sie im Inneren?
- Wärmeleitung: Ein I- oder Y-förmiges Werkstück wird an den Rändern auf konstante Temperatur beheizt. Wie verteilt sich die Wärme im Inneren? Zur Vereinfachung unterteilen wir das Werkstück in kleine Elemente. Wieder finden wir dieselben Gleichungen!

All diese Beispiele führen auf ein und dasselbe mathematische Problem, daher sind auch die Methoden und Lösungen dieselben. Abstraktion strukturiert und vereinfacht! Die Techniken funktionieren allgemeiner für endliche Graphen, bestehend aus Knoten (den Spielfeldern) und Kanten (als Verbindung zwischen Nachbarn). Google nutzt dieses Spielmodell eines zufälligen Surfers im Internet, bestehend aus Webseiten und Links, und berechnet so den *PageRank* zur Bewertung von Webseiten.

Einordnung in das Mathematikstudium. Schon an unseren Miniaturbeispielen spüren Sie, dass Ausprobieren nur in einfachen Fällen zum Erfolg führt. Vielleicht spielen Sie größer, etwa auf einem Schachbrett: Gegeben sind die 28 Randwerte, gesucht sind die Erwartungen auf den 36 inneren Feldern. Auch hier führt die Mittelwerteigenschaft zu einem linearen Gleichungssystem, allerdings größer! In physikalisch-technischen Anwendungen kommen noch größere Probleme vor, etwa 1000×2000. Spätestens jetzt benötigen wir grundlegende Theorie und praktische Algorithmen!

(1) In der **Linearen Algebra** lernen Sie im ersten Semester des Mathematikstudiums zunächst, wie Sie *lineare Gleichungssysteme* exakt lösen; die Anfänge kennen Sie schon aus der Schule. Zudem lernen Sie auch die nötige Theorie, Strukturen und Sätze, zum Beispiel handfeste Kriterien um zu erkennen, wie viele Lösungen es gibt (keine / viele / genau eine).

(2) Die **Analysis** erklärt im ersten Semester den zentralen Begriff der *Konvergenz*. Darauf bauen eine wunderbare Theorie (Grenzwertrechnung, Differenzieren, Integrieren, etc) und effiziente Methoden, zum Beispiel das Lösen von Gleichungen durch Fixpunktsätze.

(3) Was tun, wenn das Spielbrett sehr groß ist? Die Theorie garantiert eine eindeutige Lösung und liefert zudem exakte Verfahren; diese sind jedoch oft zu aufwändig. Besser nutzen Sie ein Näherungsverfahren: So berechnen Sie eine ungefähre Lösung, die zwar nicht exakt ist, aber der exakten Lösung schrittweise immer näher kommt. Die **Numerische Mathematik** entwickelt solche Algorithmen und untersucht, wie man Fehler und Aufwand klein bekommt.

(4) Unsere ursprüngliche Frage kam aus der **Wahrscheinlichkeitstheorie**. Zufällige Irrfahrten, wie in unserem Beispiel, werden als Modell für Börsenkurse genutzt (stochastische Prozesse) und ebenso in der Physik: Albert Einstein erklärte 1905 so die ungeordnete Bewegung kleiner Teilchen im Wasser durch die thermische Molekülbewegung (Brownsche Bewegung).

Stufe 3 / Mathematische Grundlage: Warum gibt es hier genau eine Lösung?

Wenn Sie bis hierher gelesen haben, dann möchten Sie vielleicht einen Vorgeschmack bekommen, was Sie im Mathematikstudium erwartet. Für alle Hartgesottenen, die es genau wissen wollen, zeigen wir hier exemplarisch einen Existenz-und-Eindeutigkeits-Satz mit Beweis. Für das Studium ist das repräsentativ. Wenn Sie die Argumente mit Geduld und Neugier sowie Stift und Papier durchgehen, können Sie ungefähr einschätzen, ob diese Art mathematischer Arbeit Ihnen Freude bereitet.

Welche Spielbretter betrachten wir? Wie zuvor sei Ω ein endliches Spielbrett, zerlegt in rote Felder R und weiße Felder W. In jedem Schritt geht man von einem weißen Feld zu einem seiner Nachbarn. Wir setzen lediglich voraus, dass von jedem weißen Feld irgendein Weg zu einem roten Feld führt.

Welche Daten sind gegeben, welche sind gesucht? In jedem roten Feld $r \in R$ ist ein Gewinn $v(r)$ vorgegeben. Gesucht ist eine Fortsetzung u auf das ganze Spielbrett Ω. Das heißt, für jedes rote Feld $r \in R$ setzen wir $u(r) = v(r)$, und für jedes weiße Feld $z \in W$ suchen wir seinen Wert $u(z)$. Dabei soll die gesuchte Fortsetzung u die Mittelwerteigenschaft in jedem weißen Feld erfüllen.

Sie kennen Minima und Maxima aus der Kurvendiskussion. Diese Begriffe sind auch hier für unser endliches Problem hilfreich: Da Ω endlich ist, nimmt u auf Ω ein Minimum an; dieses Minimum schreiben wir $\min_\Omega(u)$. Für das Minimum von u auf den roten Feldern schreiben wir $\min_R(u)$. Entsprechend schreiben wir für die Maxima $\max_\Omega(u)$ und $\max_R(u)$. Wegen $R \subset \Omega$ gilt:

$$\min_\Omega(u) \leq \min_R(u) \quad \text{und} \quad \max_\Omega(u) \geq \max_R(u)$$

Beispiel 1: Für die Lösung in Spiel 1 gilt $\min_\Omega(u) = \min_R(u) = 7$ und $\max_\Omega(u) = \max_R(u) = 23$. Alle Werte der Lösung u liegen hier also zwischen den Randwerten 7 und 23.

Beispiel 2: Für die Lösung in Spiel 2 gilt $\min_\Omega(u) = \min_R(u) = 5$ und $\max_\Omega(u) = \max_R(u) = 23$. Alle Werte der Lösung u liegen hier also zwischen den Randwerten 5 und 23.

Das ist eine bemerkenswerte Eigenschaft: In diesen Beispielen nimmt die Lösung u ihr Minimum und ihr Maximum auf dem Rand an! Wenn Sie an die Interpretation von u als Gewinnerwartung denken, dann ist das auch vollkommen plausibel. Diese Eigenschaft gilt ganz allgemein und ist eine Konsequenz der Mittelwerteigenschaft. Wir formulieren diese Aussage präzise als Satz:

Satz A: (Minimum-Maximum-Prinzip) Erfüllt die Funktion u auf dem Spielbrett Ω die Mittelwerteigenschaft, dann nimmt sie ihr Minimum und ihr Maximum auf den roten Feldern an:

$$\min_\Omega(u) = \min_R(u) \quad \text{und} \quad \max_\Omega(u) = \max_R(u).$$

Beweis: Wir betrachten zunächst das Minimum. Sei $z \in \Omega$ ein Spielfeld, in dem u sein Minimum annimmt, es gilt also $u(z) \leq u(z')$ für alle Spielfelder $z' \in \Omega$. Ist z ein rotes Feld, so sind wir fertig.

(1) Ist z ein weißes Feld, dann gilt $u(z') = u(z)$ für jedes Nachbarfeld z' von z: Dank $u(z) = \min_\Omega(u)$ gilt $u(z') \geq u(z)$. Aber $u(z') > u(z)$ ist nicht möglich, da sonst $u(z'') < u(z)$ für einen anderen Nachbarn von z nötig wäre, um die Mittelwerteigenschaft in z zu erfüllen.

(2) Wir wählen einen Weg $z, z_1, z_2, \ldots, z_n, r$ über lauter weiße Felder $z, z_1, z_2, \ldots, z_n$ bis zu einem roten Feld $r \in R$. Dank (1) gilt $u(z) = u(z_1) = u(z_2) = \cdots = u(z_n) = u(r)$ durch wiederholte Anwendung der Mittelwerteigenschaft in $z, z_1, z_2, \ldots, z_n$. Somit wird das Minimum (auch) in einem roten Feld angenommen, nämlich r. Das war zu beweisen.

Für das Maximum verläuft der Beweis genauso mit umgekehrten Ungleichungen. □

Beispiel 3: Welche Lösungen gibt es, wenn Sie $v(r) = 0$ auf jedem roten Feld $r \in R$ vorgeben? Eine mögliche Fortsetzung ist die Nullfunktion u mit $u(z) = 0$ für alle $z \in \Omega$; diese erfüllt offensichtlich die geforderte Mittelwerteigenschaft. Ist dies die einzig mögliche Lösung? Ja, dank Minimum-Maximum-Prinzip: Erfüllt irgendeine Lösung u die Mittelwerteigenschaft und $u(r) = 0$ für jedes rote Feld $r \in R$, so gilt $\min_\Omega(u) = \min_R(u) = 0$ und $\max_\Omega(u) = \max_R(u) = 0$. Somit ist u konstant Null!

Wir folgern für jede Problemstellung, dass es niemals zwei verschiedene Lösungen geben kann:

Satz B: (Eindeutigkeit) Wir geben jedem roten Feld $r \in R$ einen beliebigen Wert $v(r)$. Seien u_1 und u_2 zwei Fortsetzungen auf Ω, die beide die Mittelwerteigenschaft erfüllen. Dann gilt $u_1 = u_2$.

Beweis: Wir betrachten die Differenz $u = u_1 - u_2$. Diese erfüllt ebenfalls die Mittelwerteigenschaft. Für jedes rote Feld $r \in R$ gilt $u(r) = u_1(r) - u_2(r) = v(r) - v(r) = 0$. Wie in Beispiel 3 folgt daher $u = 0$. Das bedeutet $u_1 = u_2$. □

Es bleibt schließlich noch, die Existenz einer Lösung zu klären. Es gibt, wie Sie wissen, (inhomogene) lineare Gleichungssysteme, die keine Lösung besitzen, zum Beispiel $2x + 3y = 1$ und $4x + 6y = 3$. Wir wollen daher sicherstellen: Egal wie groß oder kompliziert das Spielbrett auch sein mag, solche Schwierigkeiten werden uns hier niemals begegnen. Das ist überaus erstaunlich und sehr erfreulich.

Satz C: (Existenz) Zu jedem Spielbrett Ω und beliebig vorgegebenen Werten $v(r)$ für jedes rote Feld $r \in R$ existiert (genau) eine Fortsetzung u auf ganz Ω, die die Mittelwerteigenschaft erfüllt.

Beweis: Je nach Vorkenntnissen wird dieser Beweis unterschiedlich lang:

(1) *Wenn Sie sich schon in der Vorlesung Lineare Algebra auskennen:*

Das vorgelegte Problem führt auf ein lineares Gleichungssystem der Form $Ax = b$. Die Matrix A ist quadratisch und kodiert das Spielbrett Ω. Der Vektor b hängt von den vorgegebenen Werten auf den roten Feldern ab. Geben Sie überall auf den roten Feldern den Wert 0 vor, so erhalten Sie das homogene System $Ax = 0$. Nach Beispiel 3 besitzt dieses System genau eine Lösung, nämlich $x = 0$. Da die Matrix A quadratisch ist, ist sie demnach invertierbar. So besitzt jede Gleichung der Form $Ax = b$ eine eindeutige Lösung, nämlich $x = A^{-1}b$. □

(2) *Wenn Sie aus der Schule den Gauß-Algorithmus beherrschen, also jedes Gleichungssystem mit Zeilenumformungen lösen können, und wissen, was in-/homogen bedeutet:*

Wir bezeichnen die weißen Felder mit $z_1, \ldots, z_n$. Die Mittelwerteigenschaft für z_i führt zu einer linearen Gleichung $a_{i1}u(z_1) + a_{i2}u(z_2) + \ldots + a_{in}u(z_n) = c_i$. So erhält man ein lineares Gleichungssystem mit n Gleichungen in den n Unbestimmten $u(z_1), u(z_2), \ldots, u(z_n)$. Ändert man die vorgegebenen Werte auf den roten Feldern, dann ändern sich lediglich die Zahlen c_i auf der rechten Seite.

(2a) Wenn Sie auf den roten Feldern überall 0 vorgeben, wie in Beispiel 3, dann sind alle $c_i = 0$. Es handelt sich um ein homogenes lineares Gleichungssystem. Aus Beispiel 3 wissen wir bereits, dass es in diesem Spezialfall genau eine Lösung gibt. Bringen Sie in diesem Fall das Gleichungssystem mit Zeilenumformungen in Zeilenstufenform, dann erhalten Sie am Ende n nichttriviale Gleichungen, denn andernfalls gäbe es mehrere Lösungen. Das heißt, die Gleichungen in (reduzierter) Zeilenstufenform sind $u(z_1) = 0$, $u(z_2) = 0$, …, $u(z_n) = 0$.

(2b) Was ändert sich nun, wenn auf den roten Feldern nicht unbedingt 0 steht, sondern beliebige Werte? Die rechte Seite c_i ist dann nicht mehr unbedingt 0, es handelt sich also um ein inhomogenes lineares Gleichungssystem. Um dieses System zu lösen, wenden Sie *dieselben* Zeilenumformungen wie in (2a) an, nur die rechte Seite ist anders. Schließlich erhalten Sie die Gleichungen $u(z_1) = c'_1$, $u(z_2) = c'_2$, …, $u(z_n) = c'_n$ und damit eine eindeutige Lösung Ihres Gleichungssystems. □

Bemerkung: Die Lösung in (2) ist lang und wortreich. Sie tut genau dasselbe wie (1). Jedoch ist (1) deutlich kürzer und klarer, denn sie nutzt die richtige Struktur: Matrizen und ihre Multiplikation. Freuen Sie sich auf die Vorlesung Lineare Algebra, in der Sie lernen, Probleme strukturiert zu lösen!

(3) *Wenn Sie lineare Gleichungssysteme per Einsetzungsverfahren, Raten oder Rumgewurschtel lösen können – zumindest manchmal:*

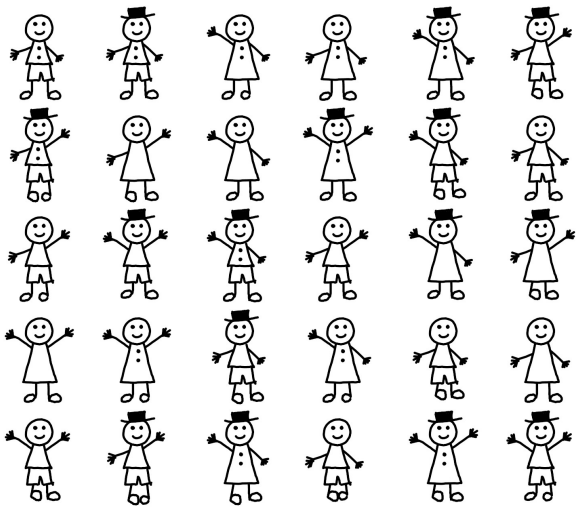
Dann wird es sicherlich schwer, diese Zusammenhänge oder überhaupt irgendetwas zu erkennen. Lineare Gleichungssysteme auf diese Art zu lösen, ist meist unstrukturiert, unnötig kompliziert und fehleranfällig. Versuchen Sie lieber, sich die Grundlagen für Methode (2) und (1) zu erarbeiten. Freuen Sie sich auf die Vorlesung Lineare Algebra, in der Sie lernen, Probleme strukturiert zu lösen!

Universität Stuttgart

Beispielaufgabe zur Studienwahl

Das doppelte Lottchen: Suchen und Sortieren

Sie machen ein Praktikum bei einer Versicherung. Jeder der 10 Millionen Kunden hat eine 15-stellige Kundennummer und weitere Versicherungsdaten, die in einer Datenbank abgespeichert sind. Diese Datenbank hat vorerst noch keine besondere Struktur, insbesondere ist sie (noch) nicht nach Kundennummern sortiert. Sie sollen überprüfen, ob alle Kundennummern wirklich verschieden sind. Dazu verwenden Sie einen Computer mit Ihrer Lieblingsprogrammiersprache. Ein Vergleich $(<, =, >)$ kostet etwa 1 Mikrosekunde, sonstige Operationen sind vernachlässigbar (Indexrechnung, nachschlagen, umordnen, etc). Beispielsweise benötigt das Auffinden der kleinsten Kundennummer $9\,999\,999$ Vergleiche und dauert etwa 10 Sekunden.



Wo ist das Doppelgängerpaar?

Wenn Sie jedes Paar auf Dopplung prüfen, wie lange benötigt der Computer?

Wie lange dauert die Prüfung auf Dopplungen, wenn die Datenbank sortiert vorliegt?

Leider ist die Datenbank völlig unsortiert. Ihre Chefin möchte dies ändern und betraut Sie mit einer möglichst effizienten Sortierung. Diese soll ebenfalls nur paarweise Vergleiche nutzen und selbst im ungünstigsten Fall möglichst schnell sein. Sie gibt Ihnen noch den Tipp, dass Sie in der Literatur oder im Internet nach bekannten vergleichsbasierten Verfahren schauen sollten.

Wie lange benötigt der Computer mit einem solchen Verfahren zum Sortieren?

Beantworten Sie jede der drei Fragen mit einem der folgenden Zeitintervalle:

unter 1 Sek.	1 bis 5 Sek.	5 bis 20 Sek.	20 bis 60 Sek.	1 bis 3 Min.	3 bis 5 Min.	5 bis 60 Min.
1 bis 24 Stunden	1 bis 7 Tage	1 bis 4 Wochen	1 bis 12 Monate	1 bis 3 Jahre	3 bis 10 Jahre	länger als 10 Jahre

mathematik fakultät8

Stufe 0 / Kurzantwort: (1) Beim Durchlaufen aller Paare führt der Computer 50 Billionen Vergleiche durch, dafür benötigt er unerträglich lange **1½ Jahre**. (2) Liegt die Datenbank bereits sortiert vor, so genügen 10 Millionen Vergleiche, also blitzschnelle **10 Sekunden**. (3) Um die Datenbank effizient zu sortieren, können wir verschiedene Algorithmen verwenden. Wir entscheiden uns hier für Mergesort (siehe `de.wikipedia.org/wiki/Mergesort` oder animiert `y2u.be/es2T6KY45cA`). Dieser Sortieralgorithmus löst unser Problem mit höchstens 240 Millionen Vergleichen. Nach spätestens 240 Sekunden, also nur **4 Minuten**, ist unsere Datenbank sortiert! Andere Verfahren liefern ähnliche Werte; im Allgemeinen geht es nachweislich nicht schneller als 218 Sekunden.

Stufe 1 / Ausführung: *Wenn Sie es genauer wissen wollen, führen wir die Rechnung für Sie aus.*

(1) Wie lange benötigt der Computer, um alle Paare zu vergleichen? Dazu zählen wir zunächst alle Paare. Wir haben $n = 10^7$ Einträge in unserer Datenbank. Eintrag 1 vergleichen wir mit den Einträgen $2, 3, \ldots, n$, das sind insgesamt $V_1 = 10^7 - 1$ Vergleiche. Eintrag 2 vergleichen wir mit den Einträgen $3, 4, \ldots, n$, das sind insgesamt $V_2 = 10^7 - 2$ Vergleiche. So können wir fortfahren: Eintrag k vergleichen wir mit allen folgenden Einträgen $(k+1), (k+2), \ldots, n$, dies sind insgesamt $V_k = 10^7 - k$ Vergleiche. Die Gesamtzahl aller paarweisen Vergleiche ist somit

$$V = \sum_{k=1}^{10^7-1} V_k = 9\,999\,999 + 9\,999\,998 + \cdots + 2 + 1.$$

Zur Berechnung dieser Summe gibt es einen genial-einfachen Trick, den Carl Friedrich Gauß schon als neunjähriger Schüler erkannte. Die folgende Summenformel heißt daher auch **der kleine Gauß**:

$$\begin{array}{rcrcrcrcrcrcrcr}
2V & = & 10^7\text{–}1 & + & 10^7\text{–}2 & + & 10^7\text{–}3 & + & \ldots & + & 3 & + & 2 & + & 1 \\
 & + & 1 & + & 2 & + & 3 & + & \ldots & + & 10^7\text{–}3 & + & 10^7\text{–}2 & + & 10^7\text{–}1 \\
\hline
 & = & 10^7 & + & 10^7 & + & 10^7 & + & \ldots & + & 10^7 & + & 10^7 & + & 10^7
\end{array}$$

Somit gilt $2V = 10^7(10^7 - 1)$, also aufgelöst

$$V = \frac{1}{2} \cdot 10^7 \cdot (10^7 - 1) = 49\,999\,995\,000\,000.$$

Alternative Betrachtung: Wie viele Vergleiche benötigen wir, wenn wir jeden Eintrag i mit *allen* anderen Einträgen $j \neq i$ vergleichen? Dies sind genau $10^7 \cdot (10^7 - 1)$ Vergleiche. Dabei behandeln wir jedoch jedes Paar $\{i, j\}$ doppelt, da wir einmal i mit j und einmal j mit i vergleichen. Somit ist die korrekte Anzahl der paarweisen Vergleiche $V = \frac{1}{2} \cdot 10^7 \cdot (10^7 - 1)$, wie oben angegeben.

Unser Computer erledigt einen Vergleich pro Mikrosekunde (10^{-6} Sekunden), also

$$\begin{aligned}
49\,999\,995\,000\,000 \cdot 10^{-6} \text{ Sek.} &= 49\,999\,995 \text{ Sek.} \\
&= 833\,333 \text{ Min. und } 15 \text{ Sek.} \\
&= 13\,888 \text{ Stunden, } 53 \text{ Min. und } 15 \text{ Sek.} \\
&= 578 \text{ Tage, } 16 \text{ Stunden, } 53 \text{ Min. und } 15 \text{ Sek.} \\
&= 1 \text{ Jahr, } 213 \text{ Tage, } 16 \text{ Stunden, } 53 \text{ Min. und } 15 \text{ Sek.}
\end{aligned}$$

Die Rechenzeit mit diesem (allzu naiven) Verfahren ist also **1 bis 3 Jahre**. Ihr Praktikum dauert sicher nicht lange genug, um das Ergebnis abzuwarten. Für Sie (und Ihre Chefin) lohnt es sich, dieses Problem rechtzeitig zu erkennen! Sie sollten Ihre Zeit besser investieren und sich ein effizienteres Verfahren überlegen. Denken hilft: Die Geschwindigkeit des Computers hängt nicht nur an der Hardware, sondern auch und vor allem an der Intelligenz / Ausbildung / Erfahrung des Benutzers!

(2) Wie lange dauert die Suche nach Dopplungen, wenn die Datenbank sortiert vorliegt?
Angenommen, die Datenbank ist bereits nach Kundennummern aufsteigend sortiert. Dies erleichtert uns die Suche nach Dopplungen enorm: Wir müssen lediglich jeden Eintrag $k = 1, \ldots, 9\,999\,999$ mit seinem Nachfolger $(k+1)$ vergleichen. Für diese $V = 9\,999\,999$ Vergleiche benötigen wir

$$9\,999\,999 \cdot 10^{-6} \text{ Sek.} \approx 10 \text{ Sek.}$$

Als Zeitintervall aus der Aufgabenstellung sind dies **5 bis 20 Sekunden**.

(3) Wie lange benötigt der Computer zum Sortieren? Zunächst müssen Sie entscheiden, mit welchem Algorithmus die Datenbank sortiert werden soll. Hierzu gibt es vergleichsbasierte Verfahren, die selbst in den ungünstigsten Fällen recht schnell sind und keinen zusätzlichen Speicherbedarf erzeugen. Egal, welchen dieser schnellen Algorithmen Sie verwenden, das Sortieren dauert in etwa gleich lang und benötigt etwa $n\lceil\log_2(n)\rceil$ Vergleiche; dies beweisen wir anschließend in Stufe 3. Notation: Für jede reelle Zahl $x \in \mathbb{R}$ bedeutet $\lfloor x \rfloor$ Abrunden und $\lceil x \rceil$ Aufrunden zur nächsten ganzen Zahl. Konkrete Anwendung: In unserem Fall ist $n = 10^7$, also $\ell = \lceil \log_2(10^7) \rceil = \lceil 23,25 \rceil = 24$. Somit genügen 240 Millionen Vergleiche, also maximal 240 Sekunden oder 4 Minuten. Genauer benötigt Mergesort höchstens $c(n) = n \cdot \ell - 2^\ell + 1$ Vergleiche, also 3 Minuten 44 Sekunden. Andere Sortieralgorithmen liefern ähnliche Werte. Die untere Schranke sind $\log_2(n!)$ Vergleiche, also 3 Minuten 38 Sekunden. In jedem Falle ist die Antwort **3 bis 5 Minuten** richtig.

Stufe 2 / Was will und soll diese Aufgabe?

Nach der Lösung dieser Aufgabe erläutern wir als Rück- und Ausblick, warum wir diese Problemstellung mathematisch interessant finden und inwiefern sie repräsentativ ist für das Mathematikstudium.

In der Mathematik geht es oft darum, eine Aussage zu beweisen oder eine Methode zu finden, die das vorgelegte Problem löst. Im Mathematikstudium erlernen Sie dazu viele nützliche Techniken. Leider bringt dieser Erfahrungsschatz wenig, wenn Sie sich naiv für die erstbeste Methode entscheiden und diese benötigt mehr Zeit, als Sie zur Verfügung haben, etwa weil Ihr Praktikum vor Ablauf eines Jahres endet. Genauso wäre es, wenn Sie eine Liste mit 10 Millionen Datensätzen ungeschickt sortieren, etwa mit quadratischem Aufwand. Nicht nur von Hand dauert das ewig, selbst ein Computer braucht dafür mehr als ein Jahr, wie oben ausgerechnet. Hätten Sie das gedacht?

> *In fact, there were many installations in which the task of sorting was responsible for more than half of the computing time. From these statistics we may conclude that either (i) there are many important applications of sorting, or (ii) many people sort when they shouldn't, or (iii) inefficient sorting algorithms have been in common use. The real truth probably involves all three of these possibilities, but in any event we can see that sorting is worthy of serious study, as a practical matter.* (Donald E. Knuth, *The Art of Computer Programming*)

Dies illustriert eine wichtige Grundregel: Zur praktischen Umsetzung Ihrer Kenntnisse müssen Sie die möglichen Methoden gründlich verstehen und für die vorliegende Anwendung eine geeignete auswählen. Manche Probleme lösen Sie mit Stift und Papier, meist ist zudem der Computer ein willkommenes Hilfsmittel, doch Sie müssen die Möglichkeiten erkennen und nutzen. Für jede ernsthafte Anwendung ist es unerlässlich, systematisch nach effizienten Lösungen zu suchen. Hierzu bietet diese Aufgabe ein repräsentatives Beispiel, mit realistischen Zahlen und anschaulicher Interpretation.

Ausblick: Algorithmen und Datenstrukturen. Im Mathematikstudium können Sie unter vielen interessanten und nützlichen Nebenfächern auswählen. Unser Beispiel Suchen und Sortieren ist ein grundlegendes Thema der Informatik, allgemeiner der Algorithmen und Datenstrukturen. Es gibt zahlreiche Sortieralgorithmen; sie unterscheiden sich nicht nur im benötigten Zeitaufwand, schlimmstenfalls oder durchschnittlich, sondern zum Beispiel auch darin, ob sie neben paarweisen Vergleichen

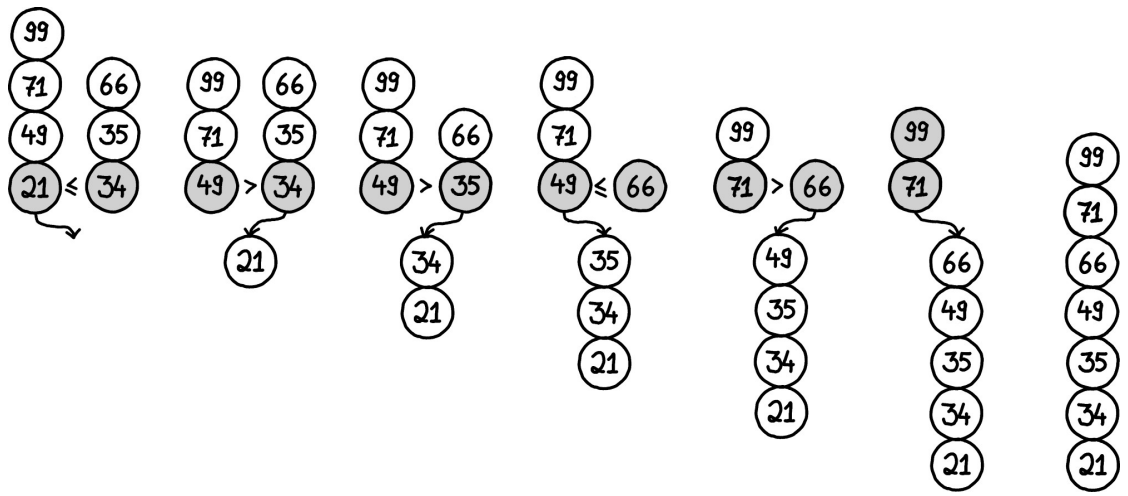
weitere Informationen verwenden, wie viel Speicherplatz sie benötigen, ob sie mit vorsortierten Listen gut umgehen oder ob sie stabil sind: Ist die Liste schon nach einem ersten Kriterium sortiert, etwa der Postleitzahl, so soll dies bei Sortierung nach weiteren Kriterien erhalten bleiben. Das hat wichtige Anwendungen! Donald E. Knuth widmet den gesamten dritten Band seines Lehrbuchs *The Art of Computer Programming* allein dem Suchen und Sortieren.

Anwendung im Beruf. Kann man mit Mathematik Geld verdienen oder ist sie eine brotlose Kunst? Tatsächlich sind die Berufsaussichten für Mathematiker:innen sehr gut: Überall, wo logisches Denken und systematisches Problemlösen gefragt sind, werden Mathematiker:innen gesucht.

Ein großes Arbeitsgebiet für Mathematiker:innen ist neben Forschung und Entwicklung, Softwareunternehmen und Unternehmensberatungen auch die Versicherungsbranche. Die Produkte einer Versicherung müssen so konzipiert sein, dass die Versicherung Gewinn macht, aber auch nicht allzu teuer ist. Vor der Einführung wird daher jedes Versicherungsprodukt genauestens überprüft, und zwar großteils von Mathematiker:innen. Es ist also nicht unwahrscheinlich, dass Sie ein Praktikum bei einer Versicherung machen. (Wenn Sie sich für ein solches Praktikum entscheiden, kann Ihnen dies im Masterstudium angerechnet werden.) Sicher werden Sie dabei auch programmieren, das gehört zum alltäglichen Handwerk und wird daher im Mathematikstudium in den ersten Semestern im Modul *Mathematische Programmierung* und später im *Computerpraktikum* erlernt und geübt. Eine Datenbank zu sortieren ist im Beruf eher eine Fingerübung zum Einstieg; bei solchen Fragen nützen Ihnen sichere theoretische Grundlagen und praktische Übung. Das zahlt sich insbesondere aus, wenn die Fragestellung kniffliger wird, und Sie nicht nach Schema F vorgehen können, sondern eigenständig die bekannten Verfahren auf neue Situationen anpassen müssen. Für Ihre Problemlösungen mit Sorgfalt und Kreativität werden Sie als Mathematiker:in gut bezahlt. Solche Praktika und scheinbar simple Probleme sind durchaus real, eine solche Geschichte wird schön erzählt in `y2u.be/RGuJga2Gl_k`.

Stufe 3 / Komplexität, obere und untere Schranken. *Wenn Sie bis hierher gelesen haben, dann möchten Sie vielleicht einen Vorgeschmack bekommen, was Sie im Studium erwartet. Wir erklären zunächst einen schnellen Sortieralgorithmus und zeigen dann, dass es nicht wesentlich schneller gehen kann. Wenn Sie die Argumente mit Geduld und Neugier sowie Stift und Papier durchgehen, können Sie ungefähr einschätzen, ob diese Art mathematischer Arbeit Ihnen Freude bereitet.*

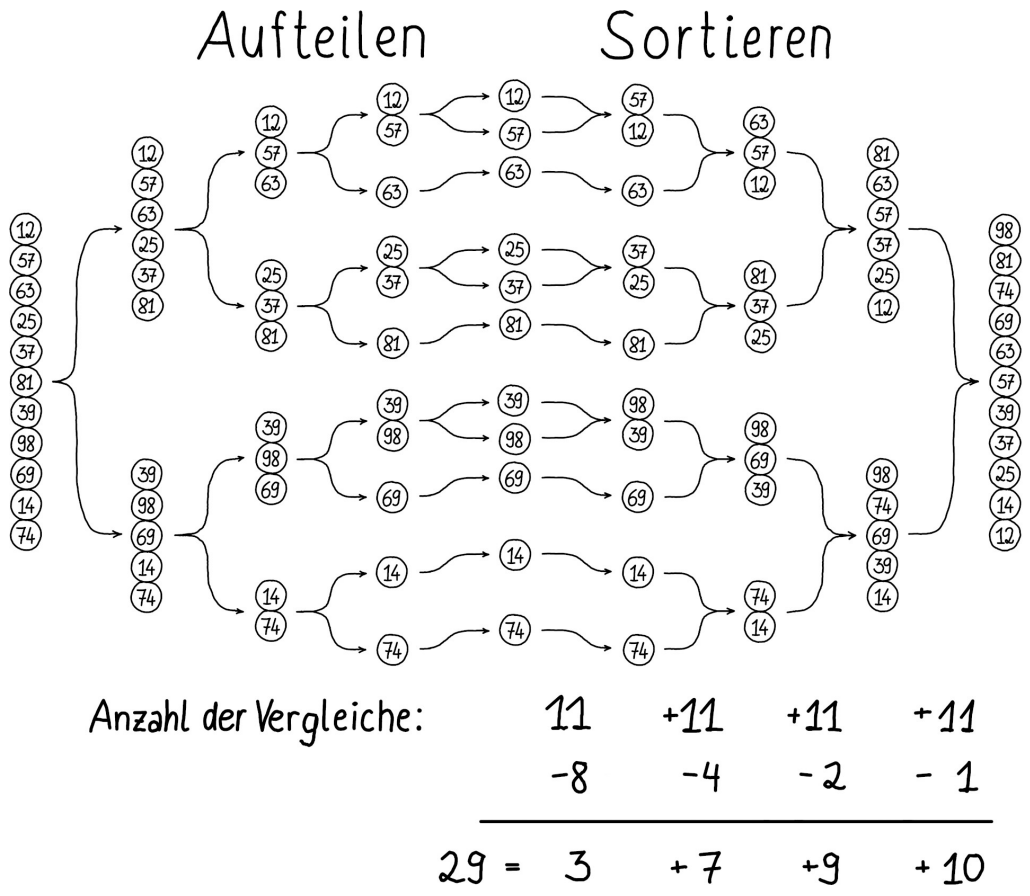
Da **Mergesort** relativ einfach und intuitiv ist, verwenden wir diesen Algorithmus: Zu sortieren ist die Liste $(A_1, A_2, \ldots, A_n)$. Im Falle $n \leq 1$ ist nichts zu tun. Im Falle $n \geq 2$ teilen wir unsere Liste mittig in zwei Listen $L = (A_1, \ldots, A_p)$ und $R = (A_{p+1}, \ldots, A_n)$ der Länge $p = \lfloor n/2 \rfloor$ und $q = \lceil n/2 \rceil$. Beide Hälften werden getrennt sortiert, und zwar rekursiv erneut mit Mergesort, und dann im Reißverschlussverfahren zusammengefügt (animiert in `y2u.be/es2T6KY45cA`).



Das Reißverschlussverfahren benötigt höchstens $p + q - 1$ Vergleiche.

Sei $c(n)$ die Anzahl der mit diesem Verfahren schlimmstenfalls ausgeführten Vergleiche. Hierzu gilt die obere Schranke $c(n) \leq n\lceil \log_2(n) \rceil$; dies wollen wir nun beweisen.

Erster Beweis: Turnier. Wie viele Vergleiche benötigen wir, um n Listeneinträge zu sortieren? Wir setzen $\ell := \lceil \log_2(n) \rceil$, sodass $2^{\ell-1} < n \leq 2^\ell$ gilt. Die Listen werden ähnlich wie bei einem Turnier in ℓ Runden vereinigt. Insgesamt finden $2^\ell - 1$ solche Vereinigungen statt, in der ersten Runde eventuell mit Listen der Länge 0. Um zwei Listen der Länge p und q zusammenzusortieren, benötigt man schlimmstenfalls $p + q - 1$ Vergleiche, also immer einen weniger als die Gesamtzahl der Listenelemente. In jeder Runde werden insgesamt n Elemente zusammensortiert. Das ergibt insgesamt $c(n) = n \cdot \ell - 2^\ell + 1$. Damit verstehen Sie insbesondere, wie diese Formel entsteht!



Sortieren als Turnier

Zweiter Beweis: Induktion. Wir wollen $c(n)$ berechnen. Wir wissen $c(0) = c(1) = 0$ und für $n \geq 2$ rekursiv $c(n) = c(\lfloor n/2 \rfloor) + c(\lceil n/2 \rceil) + n - 1$. Wir beweisen nun $c(n) = n \cdot \ell - 2^\ell + 1$ per Induktion über $n = 0, 1, 2, 3, \ldots$: Die Gleichung gilt für $n = 0$ und $n = 1$. Im Folgenden sei $n \geq 2$. Angenommen die Gleichung gilt für $c(\lfloor n/2 \rfloor)$ und $c(\lceil n/2 \rceil)$. Dann gilt sie auch für $c(n)$, denn:

$$\begin{aligned} c(n) &= c(\lfloor n/2 \rfloor) && + c(\lceil n/2 \rceil) && + n - 1 \\ &= \lfloor n/2 \rfloor (\ell - 1) - 2^{\ell-1} + 1 && + \lceil n/2 \rceil (\ell - 1) - 2^{\ell-1} + 1 && + n - 1 \\ &= n(\ell - 1) - 2^\ell + n + 1 \\ &= n\ell - 2^\ell + 1 \end{aligned}$$

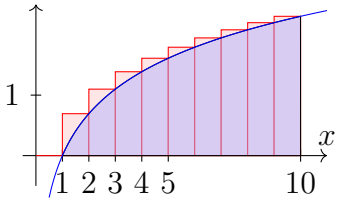
Bemerkung: Der erste Beweis durch Abzählen in einem Turnier ist kreativ und raffiniert. Der zweite Beweis nutzt die vollständige Induktion als routiniertes Handwerk. Induktion ist eine vielseitige Beweismethode und oft als konkrete Rechenmethode nutzbar, so wie hier. Wir bieten Ihnen beide Sichtweisen an: Welche finden Sie einfacher? lehrreicher? eleganter?

Untere Schranke. Wer sagt uns eigentlich, dass es nicht schneller geht? Mergesort benötigt höchstens $n\lceil\log_2(n)\rceil$ Vergleiche. Die besten bekannten vergleichsbasierten Sortieralgorithmen erfüllen alle dieselbe obere Schranke. Geht es noch besser? Können wir oder irgendjemand sonst einen noch besseren Sortieralgorithmus finden? Wir können dies mit einer unteren Schranke beantworten!

Schlimmstenfalls sind alle n Kundennummern verschieden, dann gibt es vor dem Sortieren $n!$ mögliche Anordnungen: Die erste Kundennummer kann an n verschiedenen Positionen sein, die zweite an den verbleibenden $n-1$ Positionen, usw. Das macht insgesamt $n! = n(n-1)(n-2)\cdots 2\cdot 1$ verschiedene Anfangszustände, die zu unterscheiden sind. Mit einem Vergleich kann man höchstens 2 Zustände unterscheiden, mit zwei Vergleichen höchstens 4 Zustände, mit v Vergleichen höchstens 2^v Zustände. Um also $n!$ Zustände zu unterscheiden, benötigen wir $v \geq \lceil\log_2(n!)\rceil$ Vergleiche.

Diese Zahl scheint recht groß. Wie groß genau? Rechnen wir es aus!

$$\begin{aligned}
&\ln(n!) = \ln(1\cdot 2\cdot 3\cdots(n-1)\cdot n)\\
&= \ln(1) + \ln(2) + \ln(3) + \cdots + \ln(n-1) + \ln(n)\\
&= \sum_{k=1}^{n} \ln(k) \geq \int_{x=1}^{n} \ln(x)\,\mathrm{d}x = \Big[x\ln(x) - x\Big]_{x=1}^{n} \geq n\big[\ln(n) - 1\big]
\end{aligned}$$

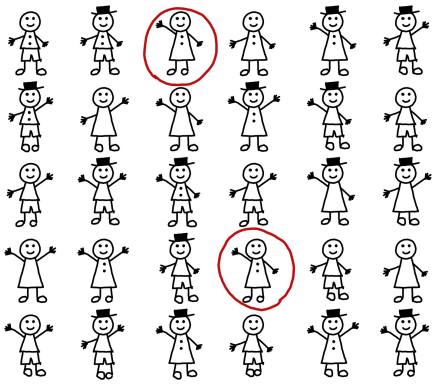


Bemerkung: (a) Die Ungleichung zwischen Summe und Integral sehen Sie, indem Sie über die Fläche des Funktionsgraphen (blau) die Summe als Balkendiagramm (rot) einzeichnen. (b) Die Stammfunktion von $\ln(x)$ können Sie durch partielle Integration finden und durch Ableiten nachprüfen.

Für $n = 10^7$ Einträge ist die Anzahl der nötigen Vergleiche also mindestens

$$\log_2(n!) = \frac{\ln(n!)}{\ln(2)} \geq \frac{n\big[\ln(n) - 1\big]}{\ln(2)} \approx 218\cdot 10^6.$$

Selbst der schnellste Algorithmus, egal ob bereits bekannt oder aktuell noch unbekannt, wird im Allgemeinen nicht schneller als 3 Minuten 38 Sekunden sein können. Wenn sich Ihre Chefin eine noch schnellere Lösung wünscht, dann können Sie ihr sachlich erklären: Die algorithmischen Möglichkeiten sind sorgfältig ausgeschöpft, ab jetzt hilft tatsächlich nur noch schnellere Hardware.



Wo ist das Doppelgängerpaar?

Und wie findet man im Suchbild die Doppelgänger?

Jede Figur mit jeder zu vergleichen, ist hier noch machbar, aber lästig. Wenn es mehr Figuren werden, wird es sehr langwierig.

Schneller geht es mit dem folgenden Verfahren: Man teilt die Figuren nach einem Merkmal auf, z.B. alle ohne Hut und alle mit Hut. In jeder der beiden Gruppen sucht man den Doppelgänger, indem man mit einem weiteren Merkmal ebenso verfährt, z.B. indem man in beiden Gruppen die Figuren mit Knöpfen und die ohne Knöpfe betrachtet. Teilt man die Gruppen immer weiter auf, so bleiben am Ende Gruppen mit einer Figur oder Gruppen aus Doppelgängern.

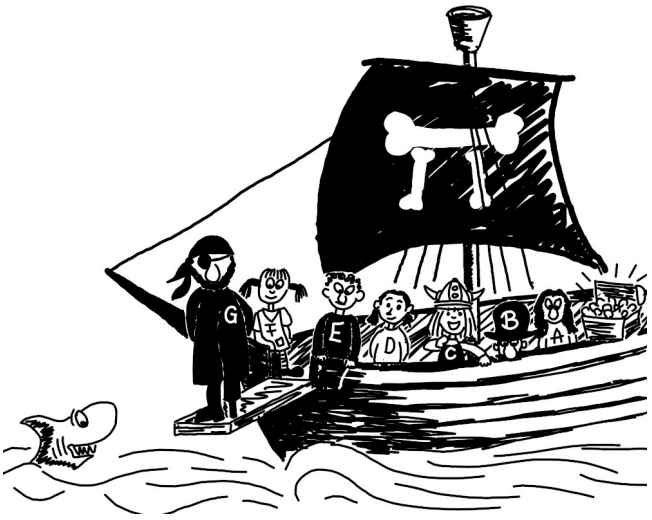
Auf dem Computer können wir dies implementieren durch einen „Fingerabdruck“ für jedes Bild: In unserem Beispiel gibt es sieben Merkmale: Kleid/Hose, mit/ohne Hut, mit/ohne Knöpfe, linke Hand, rechte Hand, linker Fuß, rechter Fuß. Dies liefert einen siebenstelligen Code, hier eine Binärzahl. Nach diesem können wir nun sortieren und so Doppelgänger finden. Dieses Verfahren, noch weiter verfeinert, wird von Google image search verwendet, um Fotos im Internet zu finden.

Universität Stuttgart

Beispielaufgabe zur Studienwahl

Mathematik auf der Bounty: das Piratenspiel

Die sieben gefürchteten Pirat:innen Anne, Bert, Charlie, Daniela, Eugen, Fabienne und Gustav teilen ihre Beute von 50 Dukaten. Der ranghöchste Pirat Gustav schlägt eine Aufteilung zur Abstimmung vor. Stimmt mindestens die Hälfte dafür, dann wird die Beute so aufgeteilt. Bei Ablehnung wird Gustav über Bord ins Meer geworfen, und die verbleibenden Pirat:innen beginnen das Spiel von vorn. Dabei gilt die Rangordnung Gustav, Fabienne, Eugen, Daniela, Charlie, Bert, Anne.



Ein Dukat ist eine unteilbare Goldmünze. Jede Pirat:in möchte überleben und möglichst viele davon haben, handelt dazu sehr schlau und vollkommen rational. Bei zwei gleichen Auszahlungen ist jede Pirat:in schadenfroh, schickt also lieber eine Kamerad:in über Bord und bevorzugt die spätere Auszahlung. Jeder weiß daher, wie die anderen handeln werden. Gleichzeitig ist jede Pirat:in sehr misstrauisch, daher sind keine Absprachen möglich. Das Leben als Pirat:in ist hart.

Wie viele Dukaten erhält jede Pirat:in? Zur Beantwortung dieser Frage lösen Sie das Problem nicht nur für sieben Pirat:innen, sondern auch für alle kleineren Fälle.

		Auszahlung an						
		Anne	Bert	Charlie	Daniela	Eugen	Fabienne	Gustav
Anzahl Pirat:innen	7							
	6							☠
	5						☠	☠
	4					☠	☠	☠
	3				☠	☠	☠	☠
	2	0	50	☠	☠	☠	☠	☠
	1	50	☠	☠	☠	☠	☠	☠

mathematik fakultät8

Stufe 0 / Kurzantwort: Die oben erklärten Regeln führen zu folgenden Aufteilungen:

		Auszahlung an						
		Anne	Bert	Charlie	Daniela	Eugen	Fabienne	Gustav
Anzahl Pirat:innen	7	**1**	**0**	**1**	**0**	**1**	**0**	**47**
	6	**0**	**1**	**0**	**1**	**0**	**48**	☠
	5	**1**	**0**	**1**	**0**	**48**	☠	☠
	4	**0**	**1**	**0**	**49**	☠	☠	☠
	3	**1**	**0**	**49**	☠	☠	☠	☠
	2	0	50	☠	☠	☠	☠	☠
	1	50	☠	☠	☠	☠	☠	☠

Das Ergebnis ist überraschend: Gustav kann tatsächlich stolze 47 Dukaten bekommen, ohne um sein Leben fürchten zu müssen. Jede Pirat:in geht planvoll vor und überlegt sich: Wie wird das enden? Daher starten wir unten in der Tabelle mit einer Piratin. Damit lösen wir das Problem für zwei Pirat:innen. Damit wiederum finden wir die Lösung für drei Pirat:innen usw. Diese geniale Methode heißt **Rekursion** oder **Rückwärtsinduktion**: Verhandelt wird vorwärts, gedacht wird rückwärts!

Stufe 1 / Ausführung: Wir betrachten die einzelnen Fälle aufsteigend in der Anzahl der Pirat:innen.

1 Piratin: Anne nimmt sich die 50 Dukaten, denn es ist niemand mehr da, mit dem sie teilen müsste oder könnte. Formal wird sie dies sich selbst vorschlagen – und natürlich dafür stimmen.

2 Pirat:innen: Der ranghöhere Bert schlägt vor: 50 Dukaten für sich, keinen für Anne. Bert stimmt dafür, Anne dagegen, weil sie bei Ablehnung mehr bekäme. Damit wird Berts Vorschlag angenommen. Das ist für ihn eindeutig das beste Vorgehen: Mit jedem anderen Vorschlag bekäme er weniger Dukaten. Wenn er gar gegen seinen eigenen Vorschlag stimmt, geht er über Bord!

3 Pirat:innen: Der ranghöchste Charlie schlägt vor: 49 Dukaten für sich, keinen für Bert, einen für Anne. Bert stimmt sowieso gegen jeden Vorschlag, weil er bei Ablehnung 50 Dukaten bekäme und zudem jemand über Bord ginge. Charlie stimmt natürlich dafür, Anne ebenso, weil sie bei Ablehnung nichts bekäme, und ein Dukat ist besser als keiner. Also wird Charlies Vorschlag mit zwei von drei Stimmen angenommen. Für Charlie ist dieser Vorschlag optimal. Berts Zustimmung bekommt Charlie ohnehin nie. Annes Zustimmung bekommt Charlie nur, wenn sie mindestens einen Dukaten erhält. Also sind 49 Dukaten für Charlie das beste Ergebnis.

4 Pirat:innen: Die ranghöchste Daniela schlägt vor: 49 für sich, 1 für Bert. Charlie und Anne stimmen dagegen, denn bei Ablehnung bekämen beide mehr. Daniela und Bert stimmen dafür, denn bei Ablehnung bekämen beide weniger. Also wird Danielas Vorschlag mit zwei von vier Stimmen angenommen. Für Daniela ist dieser Vorschlag optimal. Sie muss eine weitere Stimme gewinnen. Am günstigsten ist Bert für 1 Dukaten, Anne bräuchte 2, Charlie sogar 50.

5 Pirat:innen: Der ranghöchste Eugen benötigt neben seiner eigenen noch zwei weitere Stimmen. Die günstigsten sind Charlie und Anne für je einen Dukaten. Bert bräuchte 2, Daniela sogar 50. Also schlägt Eugen die Aufteilung 1,0,1,0,48 vor, und dieser Vorschlag wird mit drei von fünf Stimmen angenommen.

Mehr Pirat:innen: Erkennen Sie nun das Muster für n Pirat:innen? Ist n gerade, so muss der Vorschlagende $\frac{n}{2}-1$ weitere Stimmen gewinnen. Ist n ungerade, so benötigt er weitere $\frac{n-1}{2}$ Stimmen für seinen Vorschlag. Genau so viele Pirat:innen würden in der nächsten Runde bei $n-1$ Pirat:innen leer ausgehen. Diese lassen sich also mit einem Dukaten überzeugen, für die anderen müsste er mindestens zwei Dukaten locker machen. Also bietet der Vorschlagende einen Dukaten für jeden, der im nächsten Durchgang nichts erhalten würde.

Mit diesem rekursiven Vorgehen können wir alle Fälle bis 102 Pirat:innen lösen. Mathematik wirkt!

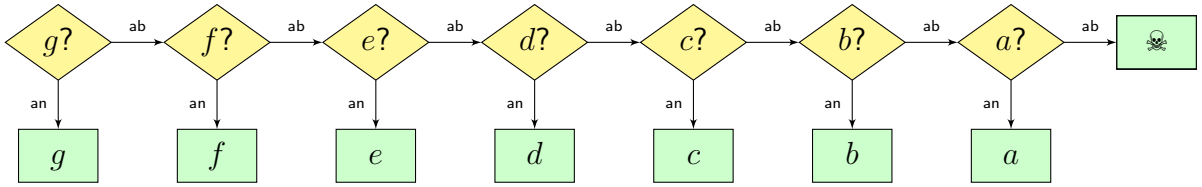
Stufe 2 / Was will und soll diese Aufgabe?

Nach der Lösung dieser Aufgabe erläutern wir als Rück- und Ausblick, warum wir diese Problemstellung mathematisch interessant finden und inwiefern sie repräsentativ ist für das Mathematikstudium.

Als vernunftbegabte Wesen wollen wir möglichst vorausschauend und planvoll handeln. Zwei hervorragende Werkzeuge hierzu sind fundierter Sachverstand und mathematische Sorgfalt.

1. Wir benötigen (a) präzise Daten und Spielregeln und (b) genaues Verständnis des Verhaltens, um das Wesentliche zu erfassen und daraus ein mathematisches Modell zu bilden.
2. Wir benötigen geeignete mathematische Werkzeuge zur Lösung des Modells.

Das ist ein allgemeines Prinzip für erfolgreiche Anwendungen der Mathematik. Wir illustrieren dies mit unserem Piratenspiel. Zur Lösung gehört als erstes der genaue Ablauf der Verhandlungen:



(1a) Rahmenvorgaben / Spielregeln: Zunächst schlägt Gustav eine Aufteilung $g = (g_1, \dots, g_7) \in \mathbb{N}^7$ mit $g_1 + \cdots + g_7 = 50$ zur Abstimmung vor. Bei Annahme bekommt Pirat $i \in \{1, \dots, 7\}$ genau g_i Dukaten ausbezahlt. Bei Ablehnung geht Gustav über die Planke und die Verhandlung in die nächste Runde. Nun schlägt Fabienne eine Aufteilung $f = (f_1, \dots, f_6, ☠)$ mit $f_1 + \cdots + f_6 = 50$ vor. Bei Annahme bekommt Pirat $i \in \{1, \dots, 6\}$ genau f_i Dukaten ausbezahlt. Bei Ablehnung geht auch Fabienne über die Planke und die Verhandlung in die nächste Runde. Nun schlägt Eugen eine Aufteilung $e = (e_1, \dots, e_5, ☠, ☠)$ mit $e_1 + \cdots + e_5 = 50$ vor, usw.

(1b) Individuelle Zielsetzung und Verhalten: Jeder Pirat (m/w/d) entscheidet nach klaren Regeln. Er bewertet sein Ergebnis gemäß $☠ < 0 < 1 < \cdots < 50$. Bei Gleichstand zwischen zwei Angeboten wird das spätere Angebot bevorzugt. Diese Informationen entnehmen wir aus der Aufgabenstellung; sie sind entscheidend, um das Verhalten der Piraten vorhersehen und somit berechnen zu können. Kurzum: Die Piraten sind vollkommen berechnend und damit selbst vollkommen berechenbar!

(2) Damit haben wir unser Modell festgelegt und können es nun mit mathematischer Sorgfalt lösen. In unserem Beispiel gelingt dies durch Rekursion bzw. (Rückwärts-)Induktion, wie in Stufe 1 erklärt. Die Wahl dieser Vorgehensweise, rückwärts zu denken, ist schon eine erste wichtige Erkenntnis. Die Diskussion jeder einzelnen Runde erfordert ebenfalls einen gewissen Aufwand, denn in jedem Schritt müssen alle Alternativen erwogen und verglichen werden. Wenn wir dabei Alternativen übersehen, müssen wir fürchten, dass es noch bessere Lösungen gibt, die uns entgehen. Sorgfalt zahlt sich aus!

Wie nützlich ist unser Modell? Unsere Beispielaufgabe klingt zunächst rein fiktiv und vollkommen praxisfern. Bei genauerer Überlegung stellt sich das Gegenteil heraus! Viele Verhandlungssituationen im Alltag, Politik, Wirtschaft, etc. sind von ähnlicher Art: Mehrere Akteure interagieren über mehrere Runden und müssen ein gemeinsames Ergebnis erzielen, zum Beispiel eine Aufteilung von Gütern und Geld, Rechten und Pflichten, etc. Unser Piratenspiel ist dazu ein gutes **Lehrbeispiel**.

Daten ändern sich, Methoden bleiben bestehen. Die hier illustrierte rekursive Vorgehensweise ist universell nutzbar: Wir lösen zunächst kleine Fälle und bauen daraus schrittweise größere Lösungen zusammen. Dieses Vorgehen ist bereits bei vielen Alltagsproblemen natürlich und nützlich, systematisch genutzt und zu einer Theorie ausgebaut wird es in der Mathematik und in der Informatik.

Zur strategischen Analyse kommt es auf die genauen Spielregeln (1a) und individuellen Zielsetzungen (1b) an. Aus solchen Fragestellungen hat sich die **Spieltheorie** entwickelt; sie untersucht ganz allgemein menschliche Interaktionen, Konflikt und Kooperation. Das Ergebnis jedes Spielers hängt dabei nicht nur von seinem eigenen Handeln ab, sondern auch von den Aktionen aller anderen.

Dafür interessieren sich nicht nur Spielbegeisterte, sondern ganz besonders Anwender in den Wirtschaftswissenschaften, in den letzten Jahrzehnten auch in vielen weiteren Gebieten, von Sozialwissenschaften bis zu Informatik. Die Lösungsmethoden (2) umfassen ein großes Spektrum mathematischer Werkzeuge. Wer Mathematik beherrscht, ist dafür bestens vorbereitet.

Wie praxistauglich ist unser Modell? Als Lehrbeispiel ist unsere Aufgabe sicher nützlich, denn wir können daran die sorgfältige Analyse (2) illustrieren. Hilft es auch in der Praxis? Ist es eine brauchbare *Vorhersage* für den Spielverlauf oder gar eine hilfreiche *Anleitung* für erfolgreiches Verhandeln?

Wir können unsere Theorie mit Experimenten vergleichen! Wenn Sie möchten, können Sie mit ein paar Versuchspersonen die obigen Verhandlungen als Rollenspiel oder Partyvergnügen durchführen – natürlich abgemildert, ohne Haie! Die empirischen Ergebnisse sind erstaunlich vielfältig und hängen von vielen Faktoren ab: Temperament, Bedenkzeit, moralischen Überzeugungen, mathematischen Kenntnissen, und vielem mehr. Manchmal ähnelt das beobachtete Verhalten der theoretischen Vorhersage, aber häufig weicht es überraschend stark davon ab.

Ist unsere Analyse also falsch? Sicher nicht! Die sorgfältige mathematische Argumentation (2) ist nachweislich richtig. Das Problem liegt in der Wahl des Modells und seiner vereinfachenden Annahmen. Die Spielregeln (1a) sind hier klar, aber die individuellen Zielsetzungen (1b) im Modell entsprechen oft nicht dem Verhalten realer Personen. Unser Modell geht davon aus, dass jeder Spieler vollkommen rational handelt, nur seinen Profit in Dukaten maximieren will, und alle Auswirkungen seines Handelns präzise erkennt. Das sind einschränkende Annahmen und Vereinfachungen!

Welche Abweichungen von dieser Idealisierung sind denkbar? Manchen Mitspielern ist nicht nur die eigene Auszahlung in Dukaten wichtig, sondern auch das Team, die Gerechtigkeit, die Moral, etc. Andere Mitspieler können die Auswirkungen ihres Handelns nur wenige Schritte voraussehen und deshalb ihre Aktionen nur eingeschränkt optimieren. Alle sind voneinander abhängig und müssen ihr Verhalten gegenseitig einschätzen. Das macht die Lage sehr kompliziert, zum Beispiel könnte ein Spieler bluffen, sich dumm stellen oder irrational handeln, um einen höheren Profit zu erpressen. Das alles bildet unser Modell (1b) noch nicht ab, und ist daher nur eingeschränkt anwendbar.

Reales menschliches Verhalten beruht nicht nur auf Vernunft und Planung, sondern häufig auf Bauchgefühl und Erfahrung, auf Versuch und Irrtum. Es ist schwierig, dafür geeignete Modelle und Vorhersagen zu finden; mit dieser Problematik beschäftigt sich die Verhaltensökonomik.

In extremen Fällen muss der erste und einzige Versuch gelingen! Große Firmen investieren daher enormen Aufwand in vorausschauende Planung, im Idealfall kommt dies der Rationalität (1b) schon recht nahe. Das erklärt auch, warum Mathematik dort eine besonders wichtige Rolle spielt.

Stufe 3 / Ausblick: Meuterei auf der Bounty – der Kampf ums Überleben

Was passiert bei einer großen Anzahl n von Piraten? Unsere Lösung aus Stufe 1 gilt bis $n = 102$: **Pirat 100** gibt den Piraten $2, 4, 6, \ldots, 100$ je einen Dukat, den anderen nichts. **Pirat 101** gibt den Piraten $1, 3, 5, \ldots, 99$ je einen Dukat, den anderen nichts. **Pirat 102** gibt den Piraten $2, 4, 6, \ldots, 100$ je einen Dukat, den anderen nichts. **Pirat 103** hat ein Problem: Jeder seiner Vorschläge wird abgelehnt, und er muss über die Planke. **Pirat 104** gibt 50 Habenichtsen aus Runde 102 je einen Dukat, den anderen nichts. So bekommt er deren 50 Stimmen, dazu die von Pirat 103 und seine eigene. Hierzu präzisieren wir eine weitere Verhaltensregel: Jeder Pirat besticht lieber rangniedrige Mitpiraten als ranghohe, also besticht Pirat 104 die Mitpiraten $1, 3, 5, \ldots, 99$. **Pirat 105** hat keine Chance, ebenso wenig 106 und 107. **Pirat 108** gibt den Piraten $2, 4, 6, \ldots, 100$ je einen Dukat, den anderen nichts. So bekommt er deren 50 Stimmen, dazu die der hoffnungslosen Piraten 105 bis 107.

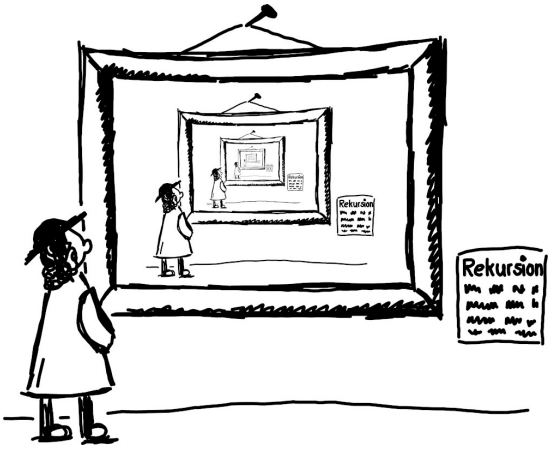
Daran erkennen wir die allgemeine Regel: Bei mehr als 100 Piraten geht es nur noch ums Überleben. Vorschlagen und dabei überleben können nur die Piraten $n = 100 + 2^k$ für $k = 0, 1, 2, \ldots$. Übung!

Universität Stuttgart

Beispielaufgabe zur Studienwahl

Rekursion und Prüfziffer: Rechnen mit Resten

© Michael Eisermann, Friederike Stoll



Wir definieren die Folge $f_0, f_2, f_2, \ldots$ ganzer Zahlen durch ihre Startwerte $f_0 = 0$ und $f_1 = 2$ sowie die rekursive Vorschrift $f_n = 3f_{n-1} - f_{n-2}$ für alle $n \geq 2$.

Berechnen Sie die ersten sechs Folgenterme:

$f_0 =$ ☐ $f_1 =$ ☐ $f_2 =$ ☐

$f_3 =$ ☐ $f_4 =$ ☐ $f_5 =$ ☐

Berechnen Sie die letzte Dezimalziffer z_n von f_n:

$z_0 =$ ☐ $z_1 =$ ☐ $z_2 =$ ☐ $z_3 =$ ☐ $z_4 =$ ☐ $z_5 =$ ☐

$z_6 =$ ☐ $z_7 =$ ☐ $z_8 =$ ☐ $z_9 =$ ☐ $z_{10} =$ ☐ $z_{11} =$ ☐

Das Programm `rechneronline.de/summe/rekursion.php` behauptet $f_{39} = 17888788647582926$. Ist das korrekt?

- ☐ Ja, weil ich es nachgerechnet habe.
- ☐ Ja, weil die erste Ziffer richtig ist.
- ☐ Ja, weil die letzte Ziffer richtig ist.
- ☐ Nein, weil die erste Ziffer falsch ist.
- ☐ Nein, weil die letzte Ziffer falsch ist.
- ☐ Nein, weil diese Zahl keine Primzahl ist.

Bestimmen Sie die letzte Ziffer von f_p für $p = 12345678$: $z_p =$ ☐

Bestimmen Sie die letzte Ziffer von f_q für $q = 3^{3^{3^3}}$: $z_q =$ ☐

mathematik fakultät8

Stufe 0 / Kurzantwort: Die gesuchten Folgenterme sind $f_0 = 0$, $f_1 = 2$, $f_2 = 6$, $f_3 = 16$, $f_4 = 42$, $f_5 = 110$ und deren letzte Ziffern $z_0 = 0$, $z_1 = 2$, $z_2 = 6$, $z_3 = 6$, $z_4 = 2$, $z_5 = 0$, $z_6 = 8$, $z_7 = 4$, $z_8 = 4$, $z_9 = 8$, $z_{10} = 0$ und $z_{11} = 2$. Danach wiederholen sich die letzten Ziffern alle zehn Folgenterme. Um z_n zu bestimmen, genügt es daher, die letzte Ziffer von n zu kennen.

Demnach endet f_{39} genauso wie f_9 mit der Ziffer $z_{39} = z_9 = 8$. Der vom Programm berechnete Wert kann nicht richtig sein, da er auf die letzte Ziffer 6 endet. Für $p = 12345678$ finden wir ebenso $z_p = z_8 = 4$. Die Zahl q endet auf 7, also gilt $z_q = z_7 = 4$.

Stufe 1 / Ausführung: Sie können die letzte Ziffer z_n auf verschiedenen Wegen berechnen; einige Rechenwege sind spürbar länger und mühsamer, andere sind geschickter und effizienter. Auch das ist Mathematik: Wir wollen nicht nur das korrekte Ergebnis, sondern auch einen effizienten Rechenweg! Der hier verwendete Trick heißt „Rechnen mit Restklassen“ oder „Modulo-Rechnung“. Im Folgenden erfahren Sie, wie das funktioniert und welche mathematischen Überlegungen dahinter stehen.

Berechnung von $f_0, \dots, f_5$: Die Folgenterme werden durch Einsetzen nacheinander berechnet:

$$f_0 = 0,\ f_1 = 2,\ f_2 = 3f_1 - f_0 = 6 - 0 = 6,\ f_3 = 16,\ f_4 = 42,\ f_5 = 110$$

Um die letzten Ziffern der Folgenterme zu berechnen, haben wir mehrere Möglichkeiten:

Mit brutaler Gewalt: Wir berechnen auch noch $f_6, \dots, f_{11}$ und nehmen dann die letzten Ziffern. Das ist mühsam, aber für die ersten Folgenterme von Hand noch machbar. Für z_{39} ist dies gerade noch möglich, aber schon lästig, für z_p mit $p = 12345678$ ist es menschlich unmöglich.

Mit geschlossener Formel: Wir konstruieren eine exakte geschlossene Formel für unsere Folge:

$$f_n = \frac{2}{\sqrt{5}}\left[\left(\frac{3+\sqrt{5}}{2}\right)^n - \left(\frac{3-\sqrt{5}}{2}\right)^n\right]$$

Steht die Formel erst einmal da, so können Sie sie leicht *überprüfen*. Wie Sie die Formel überhaupt erst *finden*, ist noch etwas raffinierter. Beides erklären wir ausführlich in Stufe 2.

Diese schöne Formel zeigt *näherungsweise* das Wachstumsverhalten für große n, denn die erste Potenz dominiert und beschert uns die Näherung $f_n \approx g_n := 0.894 \cdot 2.618^n$. Die Näherungswerte sind erstaunlich gut: $g_1 = 2.340\ldots$, $g_2 = 6.127\ldots$, $g_3 = 16.041\ldots$, $g_4 = 41.996\ldots$, $g_5 = 109.947\ldots$.

Die *exakte* Auswertung ist leider genauso mühsam wie zuvor und per Hand zudem fehleranfällig. Mit dieser Formel konkrete Folgenterme bis zur letzten Ziffer auszurechnen, ist nicht einfach.

Mit Modulo-Rechnung: Wir bemerken und nutzen, dass nur die letzte Ziffer z_n gesucht ist, und daher ist es gar nicht nötig, den Folgenterm f_n komplett auszurechnen. Um die letzte Ziffer z_n zu bestimmen, genügt es bereits, die vorigen letzten Ziffern z_{n-1} und z_{n-2} zu kennen.

Überlegung 1: Positivität aller Folgenterme. Nach den ersten Werten $f_0 = 0$, $f_1 = 2$, $f_2 = 6$, $f_3 = 16$, $f_4 = 42$, $f_5 = 110$ vermuten wir: $0 = f_0 < f_1 < f_2 < f_3 < \dots$, insbesondere ist f_n positiv für alle $n \geq 1$. Das können wir leicht nachrechnen: Zunächst gilt $f_0 = 0 < 2 = f_1$. Angenommen, wir haben bereits $0 = f_0 < f_1 < \cdots < f_{n-1} < f_n$. Dann folgt

$$f_{n+1} = 3f_n - f_{n-1} = 2f_n + \underbrace{f_n - f_{n-1}}_{>0} > 2f_n > f_n,$$

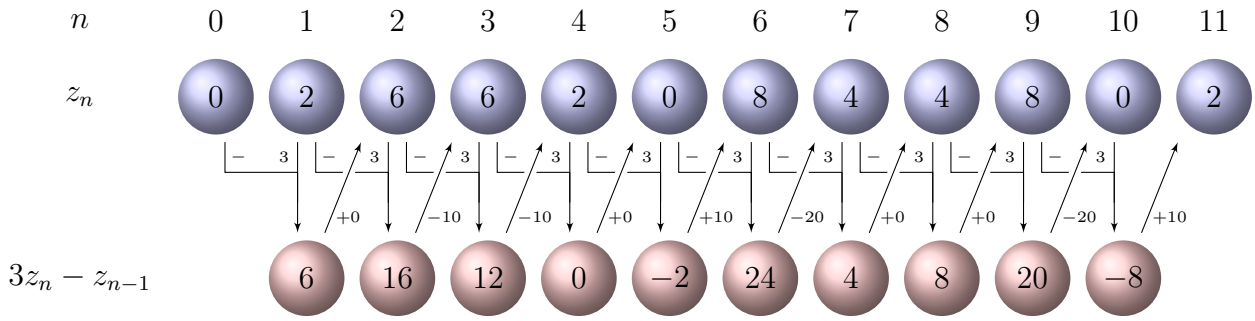
also gilt $0 = f_0 < f_1 < \cdots < f_{n-1} < f_n < f_{n+1}$. So fortfahrend erhalten wir Schritt für Schritt die vermuteten Ungleichungen $0 = f_0 < f_1 < f_2 < f_3 < \dots$, also $f_n < f_{n+1}$ für alle $n \in \mathbb{N}$.

Überlegung 2: Berechnung der letzten Ziffern. Für jede natürliche Zahl $f \in \mathbb{N}$ ist die letzte Ziffer z der Rest der Division von f durch 10. Ausgeschrieben gilt also $f = 10s + z$ mit $s, z \in \mathbb{N}$ und $0 \leq z < 10$. Allgemein dividieren wir $a \in \mathbb{Z}$ durch $b \in \mathbb{Z}$ mit $b > 0$ und erhalten $a = bs + r$ mit Quotient $s \in \mathbb{Z}$ und Rest $0 \leq r < b$. Wir schreiben kurz $r = a \operatorname{rem} b$ (engl. *remainder*).

Aus $f_{n-1} = 10s_{n-1} + z_{n-1}$ und $f_{n-2} = 10s_{n-2} + z_{n-2}$ berechnen wir

$$\begin{aligned} f_n = 3f_{n-1} - f_{n-2} &= 3 \cdot (10s_{n-1} + z_{n-1}) - (10s_{n-2} + z_{n-2}) \\ &= 10 \cdot (3s_{n-1} - s_{n-2}) + (3z_{n-1} - z_{n-2}). \end{aligned}$$

Das bedeutet $z_n = f_n \operatorname{rem} 10 = 3z_{n-1} - z_{n-2} \operatorname{rem} 10$. Anders gesagt: Wir berechnen $3z_{n-1} - z_{n-2}$ und addieren bzw. subtrahieren so oft 10, bis wir die ersehnte Ziffer $z_n \in \{0, 1, \ldots, 9\}$ erhalten.



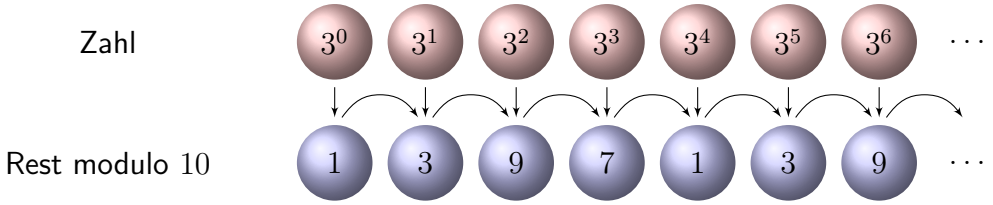
Mit diesem Trick können wir die Ziffern z_n einfacher und schneller bestimmen, sogar im Kopf!

Déjà Vu: Die letzten beiden Werte sind eine 0 gefolgt von einer 2. Das hatten wir schon ganz am Anfang! Damit beginnt alles wieder von vorne und wiederholt sich immer in Zehnerschritten: Für alle natürlichen Zahlen $n, k \in \mathbb{N}$ gilt $z_{n+10k} = z_n$. Wollen Sie also z_n ausrechnen, so genügt es, die letzte Ziffer $i = n \operatorname{rem} 10$ zu kennen, denn dann gilt $z_n = z_i$. Mit diesem Trick müssen Sie nun überhaupt nicht mehr rechnen, sondern können den Wert z_i einfach in obiger Tabelle nachschlagen!

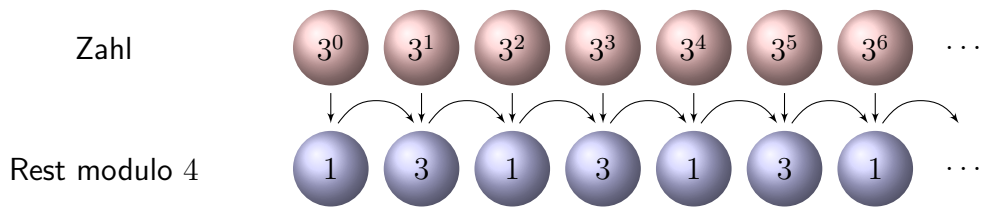
Prüfziffer: Die letzte Ziffer $z_{39} = f_{39} \operatorname{rem} 10$ lesen wir ebenso leicht ab: $z_{39} = z_9 = 8$. Dies widerspricht dem Ergebnis, das das Programm `rechneronline.de/summe/rekursion.php` liefert. So enttarnen Sie diesen (Rundungs-)Fehler: mit wenig Aufwand, aber mathematischer Finesse!

Große Zahlen: Ebenso leicht können wir $z_p = f_p \operatorname{rem} 10$ für $p = 12345678$ bestimmen: $z_p = z_8 = 4$.

Astronomisch große Zahlen: Mit demselben Trick berechnen wir $z_q = f_q \operatorname{rem} 10$ für $q = 3^{3^{3^3}}$. Dazu berechnen wir $i = q \operatorname{rem} 10$ und nutzen $z_q = z_i$. Für $n = 0, 1, 2, \ldots, 3^{3^3}, \ldots$ berechnen wir $3^n \operatorname{rem} 10$:



Diese Potenzfolge $a_n = 3^n$ entsteht durch die Rekursion $a_0 = 1$ und $a_n = 3a_{n-1}$ für $n = 1, 2, 3, \ldots$ und unsere obigen Überlegungen übertragen sich. Die letzte Ziffer $3^n \operatorname{rem} 10$ wiederholt sich alle vier Schritte. Für $n = 4k + r$ haben 3^n und 3^r dieselbe letzte Ziffer. Speziell für $n = 3^{3^3}$ wollen wir also $r = n \operatorname{rem} 4$ berechnen. Wie zuvor untersuchen wir dazu $3^m \operatorname{rem} 4$ für $m = 0, 1, 2, \ldots, 3^3, \ldots$:



Demnach gilt $3^m \operatorname{rem} 4 = 1$, falls m gerade ist, und $3^m \operatorname{rem} 4 = 3$, falls m ungerade ist. In den drei Grafiken lesen wir nun von unten nach oben ab: Da $m = 3^3$ ungerade ist, bleibt für $n = 3^m = 3^{3^3}$ der Rest $n \operatorname{rem} 4 = 3$. Also ist $q \operatorname{rem} 10 = 3^n \operatorname{rem} 10 = 7$ und daher $z_q = z_7 = 4$.

Stufe 2 / Was will und soll diese Aufgabe?

Nach der Lösung dieser Aufgabe erläutern wir als Rück- und Ausblick, warum wir diese Problemstellung mathematisch interessant finden und inwiefern sie repräsentativ ist für das Mathematikstudium.

Zunächst lernen Sie an dieser Aufgabe: Vertrauen Sie nicht blind einem Computerprogramm! Seien Sie achtsam und prüfen Sie, ob numerische Ergebnisse stimmig und sinnvoll sind. Programme machen nicht immer das, was man denkt oder wünscht. Daher ist es wichtig, Hintergründe zu kennen, Ergebnisse zu hinterfragen und auf Plausibilität zu prüfen. Im Studium lernen Sie die mathematischen Grundlagen und Methoden, um diese selbstständig, sicher, kritisch, korrekt und kreativ anzuwenden!

Hier illustrieren wir Rekursion und Induktion. **Rekursion** ist eine grundlegende Konstruktionsmethode in Mathematik und Informatik und vielen Anwendungen. Die berühmte Fibonacci-Folge zum Beispiel beschreibt die Größe a_n einer Kaninchenpopulation zur Zeit $n = 0, 1, 2, \ldots$; sie entsteht durch die Startwerte $a_0 = a_1 = 1$ und die Rekursionsvorschrift $a_n = a_{n-1} + a_{n-2}$ für alle $n \geq 2$.

Eng verbunden mit der Rekursion ist die **Induktion** als grundlegende Beweismethode. Beides sind Universalwerkzeuge, die Sie daher gleich zu Beginn des Studiums erlernen. Die Rekursion dient zur Konstruktion einer Folge, die Induktion dient zum Nachweis einer Aussage. Zu zeigen ist eine

- Behauptung: Für alle natürlichen Zahlen $n \in \mathbb{N}$ mit $n \geq m$ gilt die Aussage $A(n)$.

Diese zeigen wir mittels vollständiger Induktion durch Nachweis der beiden folgenden Aussagen:

- Induktionsanfang: Es gilt die erste Aussage $A(m)$ für den vorgegebenen Startwert m.
- Induktionsschritt: Für jede natürliche Zahl $n \geq m$ gilt: Aus $A(n)$ folgt $A(n+1)$.

Die Idee ist sehr anschaulich: Es gilt $A(m)$. Daraus folgt $A(m+1)$. Daraus folgt $A(m+2)$. Daraus folgt $A(m+3)$. Und so weiter. Die sorgfältige Ausformulierung sind genau die beiden obigen Punkte: Induktionsanfang und Induktionsschritt. Zwei einfache Beispiele aus Stufe 1 sollen dies illustrieren.

Behauptung 1: Für alle $n \geq 1$ gilt die Aussage $A(n)$: $f_n > f_{n-1} \geq 0$.

Beweis: Wir nutzen das Prinzip der vollständigen Induktion.

- Induktionsanfang: Die Aussage $A(1)$ gilt, denn $f_1 = 2$ und $f_0 = 0$, also $f_1 > f_0 \geq 0$.
- Induktionsschritt: Gegeben sei $n \geq 1$ und die gültige Aussage $A(n)$, also $f_n > f_{n-1} \geq 0$. Daraus folgt $f_{n+1} = 2f_n + f_n - f_{n-1} > 2f_n > f_n > 0$. Somit gilt die Aussage $A(n+1)$. □

Bemerkung: Wichtig sind sowohl Induktionsschritt als auch Induktionsanfang. Für die Startwerte $f_0 = 3$ und $f_1 = 1$ zeigt die Folge $f_2 = 0$, $f_3 = -1$, $f_4 = -3$, usw. ein ganz anderes Verhalten!

Bemerkung: Oft wird das Prinzip der vollständigen Induktion in einer **starken Formulierung** verwendet: Eigentlich wollen wir die Aussagen $A(n)$ für alle $n \geq m$ zeigen. Dazu zeigen wir für alle $n \geq m$ die scheinbar stärkere Aussage $B(n)$: Für alle $k \in \mathbb{N}$ mit $m \leq k \leq n$ gilt $A(k)$. Das bedeutet konkret: Im Induktionsschritt folgern wir aus $A(k)$ für alle k mit $m \leq k \leq n$ die Aussage $A(n+1)$. Beide Formulierungen sind logisch äquivalent, die schwache ist sparsamer, die starke ist bequemer.

In Stufe 1 haben wir angekündigt, die geschlossene Formel zu überprüfen. Mit dem richtigen Werkzeug gelingt dies nun leicht und wir können sie für alle $n \in \mathbb{N}$ beweisen, sehr elegant und effizient.

Behauptung 2: Für alle $n \geq 0$ gilt die Aussage $A(n)$: $f_n = g_n := \frac{2}{\sqrt{5}}\left[\left(\frac{3+\sqrt{5}}{2}\right)^n - \left(\frac{3-\sqrt{5}}{2}\right)^n\right]$.

Beweis: Wir nutzen das Prinzip der vollständigen Induktion (in der starken Formulierung).

- Induktionsanfang: Die ersten beiden Aussagen $A(0)$ und $A(1)$ sind wahr, denn wir berechnen $g_0 = \frac{2}{\sqrt{5}}\left[\left(\frac{3+\sqrt{5}}{2}\right)^0 - \left(\frac{3-\sqrt{5}}{2}\right)^0\right] = \frac{2}{\sqrt{5}}(1-1) = 0$ und $g_1 = \frac{2}{\sqrt{5}}\left[\left(\frac{3+\sqrt{5}}{2}\right)^1 - \left(\frac{3-\sqrt{5}}{2}\right)^1\right] = 2$.
- Induktionsschritt: Es gelte $f_k = g_k$ für $k \leq n$. Geduldig rechnet man zuerst $g_{n+1} = 3g_n - g_{n-1}$ nach. (Versuchen Sie dies als Übung!) Nach Voraussetzung gilt $g_n = f_n$ und $g_{n-1} = f_{n-1}$, also folgt $g_{n+1} = 3g_n - g_{n-1} = 3f_n - f_{n-1} = f_{n+1}$. Somit gilt die Aussage $A(n+1)$. □

Auf der Suche nach einer geschlossenen Formel. Mit Induktion können wir die geschlossene Formel für f_n leicht nachprüfen, aber wie kommen wir auf eine solche Formel? Zufällig erraten wird man diese Formel wohl kaum. Wir suchen daher eine möglichst allgemeine Lösungsmethode!

Für die einfachere Folge $a_0 = 5$ und $a_n = 3a_{n-1}$ ist die Formel leicht zu finden: Es gilt $a_n = 5 \cdot 3^n$. Das bringt uns auf die Idee, eine Formel $f_n = \lambda \cdot b^n$ zu versuchen. Das nennt man die **Ansatzmethode**: Wir machen einen (geschickt geratenen) Ansatz und bestimmen die noch freien Parameter λ und b. Wir setzen zunächst $f_n = b^n$ in die Rekursionsgleichung $f_n = 3f_{n-1} - f_{n-2}$ ein und erhalten

$$b^n = 3b^{n-1} - b^{n-2}.$$

Es genügt, für $n = 2$ die Gleichung $b^2 = 3b - 1$ zu erfüllen, alle höheren Gleichungen folgen daraus. Für die quadratische Gleichung $b^2 = 3b - 1$ berechnen wir dank Mitternachtsformel die beiden Lösungen $b_{1/2} = \frac{3 \pm \sqrt{5}}{2}$. Wir erhalten daher zwei Lösungen der Rekursionsgleichung $g_n = \left(\frac{3+\sqrt{5}}{2}\right)^n$ und $h_n = \left(\frac{3-\sqrt{5}}{2}\right)^n$. Leider erfüllt keine der beiden unsere Anfangsbedingungen $f_0 = 0$ und $f_1 = 2$.

Sind wir gescheitert? Hier rettet uns **Linearität**: Auch jede Linearkombination $f_n = \lambda g_n + \mu h_n$ mit $\lambda, \mu \in \mathbb{R}$ erfüllt die Rekursionsgleichung. Können wir λ und μ so wählen, dass unsere Anfangsbedingungen erfüllt sind? Für $n = 0$ muss $f_0 = 0$ gelten, also $\lambda + \mu = 0$. Für $n = 1$ muss $f_1 = 2$ gelten, also $\lambda b_1 + \mu b_2 = 2$. Dieses lineare Gleichungssystem hat die eindeutige Lösung $\lambda = \frac{2}{\sqrt{5}}$, $\mu = -\frac{2}{\sqrt{5}}$. (Übung!) Wir erhalten so die ersehnte geschlossene Formel:

$$f_n = \tfrac{2}{\sqrt{5}}\left[\left(\tfrac{3+\sqrt{5}}{2}\right)^n - \left(\tfrac{3-\sqrt{5}}{2}\right)^n\right]$$

Alternativ erhalten Sie die geschlossene Formel mit Matrizenrechnung und Diagonalisierung. Wie das genau funktioniert, lernen Sie im ersten Studienjahr in der Vorlesung **Lineare Algebra**.

Stufe 3 / Mathematische Grundlage: Modulo-Rechnung.

Das Rechnen mit Resten, kurz Modulo-Rechnung, ist überall nützlich. In unserem Beispiel haben wir mit der „Prüfziffer“ leicht nachgewiesen, dass das Computerprogramm falsch gerechnet hat. Modulo-Rechnung spielt ebenso in der **Kryptographie** eine zentrale Rolle. Das klassische RSA-Verfahren und viele nachfolgende asymmetrische Verschlüsselungsverfahren, basieren auf Modulo-Rechnung.

Beim Lösen der Aufgabe haben wir beobachtet, dass es reicht, nur auf die letzten Ziffern zu achten, also auf die Reste bei Division durch 10. Später wurden Reste bei Division durch 4 bzw. durch 2 betrachtet. Dies kann man mathematisch genauer beschreiben, formalisieren und verallgemeinern:

Wir fixieren eine natürliche Zahl $m \in \mathbb{N}_{\geq 1}$. Wir nennen zwei ganze Zahlen a und b *kongruent modulo* m, geschrieben $a \equiv b \pmod{m}$, falls ihre Differenz $a - b$ durch m teilbar ist, und zwar ganzzahlig ohne Rest. Die Bedingung $a \equiv b \mod m$ ist äquivalent zu $a \operatorname{rem} m = b \operatorname{rem} m$.

Beispiel: Modulo $m = 7$ gilt $1 \equiv 8$, $2 \equiv 23$ und $-11 \equiv 3$. Die Präzisierung $\mod 7$ lassen wir weg.

Alle Zahlen, die zu $a \in \mathbb{Z}$ kongruent modulo m sind, wollen wir zusammenfassen und wie ein einziges Element behandeln: Die Kongruenzklasse $[a] := \{\, b \in \mathbb{Z} \mid a \equiv b \pmod{m} \,\}$ ist die Menge aller ganzen Zahlen b, die zu a kongruent sind. Genau dann gilt $[a] = [b]$, wenn $a \equiv b \pmod{m}$ ist.

Beispiel: Modulo $m = 10$ erhalten wir genau zehn verschiedene Kongruenzklassen:

$$\begin{aligned}
[0] &= \{\ldots, -20, -10,\ \ 0, 10, 20, \ldots\}, \\
[1] &= \{\ldots, -19,\ \ -9,\ \ 1, 11, 21, \ldots\}, \\
&\ldots, \\
[9] &= \{\ldots, -11,\ \ -1,\ \ 9, 19, 29, \ldots\}.
\end{aligned}$$

Jede ganze Zahl a gehört zu genau einer dieser Kongruenzklassen, nämlich zu $[a \operatorname{rem} 10]$.

Allgemein erhalten wir die Menge $\mathbb{Z}/m = \{\,[0],[1],\ldots,[m-1]\,\}$ aller Kongruenzklassen von $\mathbb{Z}$ modulo m. Kongruenzklassen können wir addieren durch $[a]+[b] := [a+b]$ und multiplizieren durch $[a]\cdot[b] := [a\cdot b]$. In Worten: Um zwei Kongruenzklassen zu verknüpfen, wählen wir daraus je ein Element a und b, verknüpfen diese, und bilden dazu die Kongruenzklasse. Hierbei ist Vorsicht geboten, denn wir müssen willkürlich Elemente wählen, und es ist keineswegs klar, ob das Ergebnis von unseren Wahlen abhängt. Das tut es wundersamerweise nicht! Hier einige Beispiele:

In $\mathbb{Z}$ gilt	$67+34=101,$	$67\cdot 34=2278,$
	$(-3)+24=21,$	$(-3)\cdot 24=-72,$
	$17+(-6)=11,$	$17\cdot(-6)=-102.$
In $\mathbb{Z}/10$ gilt	$[7]+[4]=[1],$	$[7]\cdot[4]=[8].$

Allgemein müssen wir folgendes nachrechnen: Aus $[a]=[a']$ und $[b]=[b']$ folgt $[a+b]=[a'+b']$ und $[a\cdot b]=[a'\cdot b']$. Versuchen Sie dies als Übung! Oder freuen Sie sich auf das Mathematikstudium!

Die folgenden Tabellen zeigen Addition und Multiplikation in der Menge $\mathbb{Z}/10$:

$+$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[7]	[8]	[9]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[7]	[8]	[9]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[7]	[8]	[9]	[0]	[1]	[2]	[3]	[4]	[5]
[7]	[7]	[8]	[9]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[8]	[8]	[9]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[9]	[9]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]

$\cdot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]
[2]	[0]	[2]	[4]	[6]	[8]	[0]	[2]	[4]	[6]	[8]
[3]	[0]	[3]	[6]	[9]	[2]	[5]	[8]	[1]	[4]	[7]
[4]	[0]	[4]	[8]	[2]	[6]	[0]	[4]	[8]	[2]	[6]
[5]	[0]	[5]	[0]	[5]	[0]	[5]	[0]	[5]	[0]	[5]
[6]	[0]	[6]	[2]	[8]	[4]	[0]	[6]	[2]	[8]	[4]
[7]	[0]	[7]	[4]	[1]	[8]	[5]	[2]	[9]	[6]	[3]
[8]	[0]	[8]	[6]	[4]	[2]	[0]	[8]	[6]	[4]	[2]
[9]	[0]	[9]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

Übung: Schreiben Sie für $\mathbb{Z}/m$ mit $m=2,3,4,5$ die Additions- und Multiplikationstabelle aus.

Die Konstruktion von $\mathbb{Z}/m$ ist raffiniert und grundlegend. Was ist der Nutzen? Die neue Schreibweise für Addition und Multiplikation ist kurz und präzise und daher für Rechnungen sehr effizient. Wir illustrieren dies, indem wir unsere obigen Rechnungen kurz, präzise und elegant formulieren:

Behauptung 3: Für alle $n \geq 10$ gilt die Aussage $A(n)$: $[f_n]=[f_{n-10}]$.

Beweis: Wir nutzen das Prinzip der vollständigen Induktion (in der starken Formulierung).

- Induktionsanfang: Für $n=10$ und $n=11$ rechnet man $A(n)$ einfach nach, wie oben gezeigt.
- Induktionsschritt: Sei $n \geq 11$ und für alle k mit $10 \leq k \leq n$ gelte $A(k)$. Somit gelten die Aussagen $A(n-1)$: $[f_{n-1}]=[f_{n-11}]$ und $A(n)$: $[f_n]=[f_{n-10}]$. Damit folgt $A(n+1)$, denn $[f_{n+1}]=[3f_n-f_{n-1}]=[3][f_n]-[f_{n-1}]=[3][f_{n-10}]-[f_{n-11}]=[3f_{n-10}-f_{n-11}]=[f_{n-9}]$. □

Behauptung 4: Für alle $n \geq 0$ gilt $A(n)$: $[f_n]=[f_{n\mathrm{rem}10}]$, für die letzten Ziffern also $z_n = z_{n\mathrm{rem}10}$.

Beweis: Wir nutzen das Prinzip der vollständigen Induktion (in der starken Formulierung).

- Induktionsanfang: Die Aussage $A(n)$ gilt für $n=0,1,\ldots,9$, denn hier ist $n = n \operatorname{rem} 10$.
- Induktionsschritt: Sei $n \geq 10$ und für alle k mit $0 \leq k < n$ gelte die Aussage $A(k)$. Wir nutzen $n' = n-10 \geq 0$ und $n' \operatorname{rem} 10 = n \operatorname{rem} 10$. Dank Behauptung 3 und Induktionsvoraussetzung $A(n')$ gilt $[f_n]=[f_{n'}]=[f_{n'\mathrm{rem}10}]=[f_{n\mathrm{rem}10}]$. □

Die weiteren Rechnungen modulo 4 bzw. 2 lassen sich ebenso elegant formulieren. Versuchen Sie dies als Übung! Auch dies ist eine Stärke der Mathematik: Dank guter und präziser Notation werden unsere Rechnungen übersichtlicher und leichter. Abstraktion hilft ganz konkret!

Universität Stuttgart

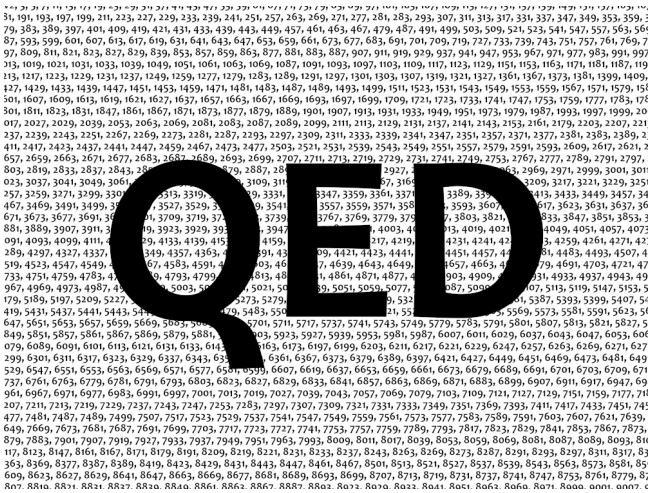
Beispielaufgabe zur Studienwahl

Wissenschaftlich geprüft: ein kleiner Beweis

Im Mathematikstudium werden Sie viele schöne und lehrreiche Beweise kennen lernen und auch selbst ausführen. Als kleinen Vorgeschmack beweisen wir einen Satz aus der Schulmathematik:

Es gibt unendlich viele Primzahlen.

Bringen Sie dazu die folgenden Beweisschnipsel in die richtige Ordnung. Die üblichen Regeln zur Teilbarkeit ganzer Zahlen werden vorausgesetzt, ebenso die Tatsache, dass jede natürliche Zahl ≥ 1 ein Produkt von Primzahlen ist.



	Position
Es gilt $p_i \neq q_j$ für alle (i, j). Andernfalls teilte nämlich $p_i = q_j$ sowohl p als auch $q = p + 1$, also auch die Differenz $q - p = 1$, und wir hätten $p_i = q_j = 1$.	☐
Daraus folgt der Satz: Es gibt unendlich viele Primzahlen.	☐
Also können wir zu den gegebenen Primzahlen $p_1, p_2, \ldots, p_n$ noch weitere, davon verschiedene Primzahlen $q_1, q_2, \ldots, q_m$ konstruieren.	☐
Zu gegebenen Primzahlen $p_1, p_2, \ldots, p_n \geq 2$ konstruieren wir mindestens eine weitere Primzahl.	☐
Wir führen einen konstruktiven Beweis:	☐
Wir zerlegen $q = q_1 \cdot q_2 \cdots q_m$ in ein Produkt von Primzahlen $q_1, q_2, \ldots, q_m \geq 2$; wegen $q \geq 2$ gilt $m \geq 1$.	☐
Wir betrachten das Produkt $p = p_1 \cdot p_2 \cdots p_n \geq 1$ und $q = p + 1 \geq 2$.	☐

mathematik fakultät8

Stufe 0 / Kurzantwort: Für diese Beweisschnipsel gibt es nur eine logisch richtige Reihenfolge:

(1) Wir führen einen konstruktiven Beweis:

(2) Zu gegebenen Primzahlen $p_1, p_2, \ldots, p_n \geq 2$ konstruieren wir mindestens eine weitere Primzahl.

(3) Wir betrachten das Produkt $p = p_1 \cdot p_2 \cdots p_n \geq 1$ und $q = p + 1 \geq 2$.

(4) Wir zerlegen $q = q_1 \cdot q_2 \cdots q_m$ in ein Produkt von Primzahlen $q_1, q_2, \ldots, q_m \geq 2$; wegen $q \geq 2$ gilt $m \geq 1$.

(5) Es gilt $p_i \neq q_j$ für alle (i, j). Andernfalls teilte nämlich $p_i = q_j$ sowohl p als auch $q = p + 1$, also auch die Differenz $q - p = 1$, und wir hätten $p_i = q_j = 1$.

(6) Also können wir zu den gegebenen Primzahlen $p_1, p_2, \ldots, p_n$ noch weitere, davon verschiedene Primzahlen $q_1, q_2, \ldots, q_m$ konstruieren.

(7) Daraus folgt der Satz: Es gibt unendlich viele Primzahlen.

Stufe 1 / Ausführung: Wie bauen wir einen Beweis richtig auf?

Wir möchten, dass unser Beweis gut lesbar ist, zum Ziel führt und dabei weder Fehler enthält noch Lücken lässt. Das erfordert viel Übung, und dabei helfen uns einige Grundregeln:

Zum guten Stil gehört die klassische Dreiteilung: Am Anfang sagen wir, was wir tun möchten, dann tun wir genau dies, und am Ende stellen wir fest, dass wir es getan haben. Das klingt redundant, trägt aber viel zu Klarheit und Lesbarkeit bei. Mathematik beruht auch auf guter Kommunikation.

Hier beginnen wir mit der Ankündigung (1) „Wir führen einen konstruktiven Beweis.“ und der präzisierten Behauptung (2); diese sagt sogar etwas mehr als der anvisierte Satz. Diese Zielsetzung gibt bereits eine erste Idee, wie die folgenden Argumente verlaufen sollen. Eine Alternative wäre zum Beispiel ein indirekter Beweis. Dann kommt als Hauptteil die eigentliche Beweisführung (3)–(6). Wir schließen mit der Zusammenfassung (7) „Daraus folgt der Satz.“ Das signalisiert, dass jetzt alles gezeigt ist und keine weiteren Ausführungen folgen.

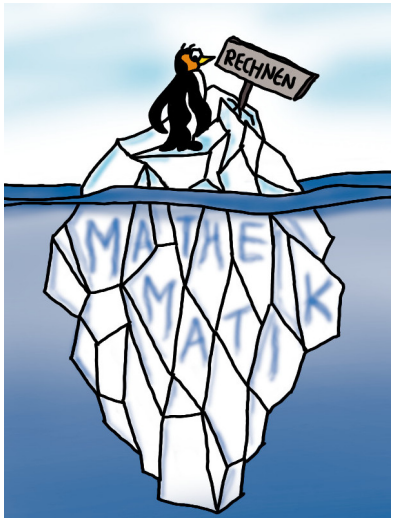
Wie bringen wir jetzt die Schritte (3)–(6) in die richtige Reihenfolge? Einfache Grundregel: Alle Bezeichnungen und Variablen, die wir verwenden, müssen wir zuvor einführen und erklären. Hier bedeutet das konkret: Aussage (6) fasst zusammen, was in (5) ausgeführt wurde. Schritt (5) benötigt Schritt (4), dieser benötigt (3), und dieser wiederum (2). Für die hier vorgegebenen Beweisschnipsel gibt es also nur eine logische Reihenfolge. Für die Anordnung allein genügt demnach bereits eine formale Syntax-Prüfung.

In der auf diese Weise *formal* gefundenen Reihenfolge können wir die Beweisschritte nun *logisch* überprüfen. Hier gilt die einfache Grundregel: Jeder Beweisschritt darf nur verwenden, was zuvor bereits gezeigt oder konstruiert wurde, und leitet daraus weitere Aussagen oder Konstruktionen direkt ab. Das können Sie im obigen Beweis nun sorgfältig Schritt für Schritt nachprüfen! Das Ergebnis ist eine lückenlose Argumentationskette. Als Ziel haben wir anfangs die Behauptung (2) formuliert. Diese wird in den folgenden Schritten (3), (4), (5) hergeleitet und in (6) erreicht.

Die vereinfachende Zusammenfassung (7) folgt direkt aus (6).

Stufe 2 / Was will und soll diese Aufgabe?

Nach der Lösung dieser Aufgabe erläutern wir als Rück- und Ausblick, warum wir diese Problemstellung mathematisch interessant finden und inwiefern sie repräsentativ ist für das Mathematikstudium.



Schulmathematik besteht leider allzu oft nur aus sturem Anwenden von fertigen Rezepten und stupidem Auswendiglernen von Formeln und Algorithmen. Im Extrem wird sinnentleerte Formelgläubigkeit praktiziert: „Hier sind Zahlen x und y, setze sie in die magische x–y–Formel ein!“ Das vermittelt weder solide Grundlagen, noch bereitet es auf ernsthafte Anwendungen vor: Blindes Anwenden ohne Verstehen ist gefährlich! Die handwerklich routinierte Ausführung ist durchaus wichtig, aber eben nur ein sehr kleiner Teil der Wahrheit.

Echte Mathematik ist viel umfassender und interessanter!

- Zu vielen Problemen sind noch gar keine Lösungen bekannt! Fertige Rezepte und stures Auswendiglernen helfen hier kein Stück weiter. Gefragt sind im Gegenteil Kreativität, Umsicht und Einfallsreichtum, um überhaupt erst geeignete Methoden zu finden, maßgeschneiderte Algorithmen zu entwickeln, oder bekannte Ergebnisse anzupassen.
- Meist geht es nicht nur um einzelne Beispiele, das wäre hoffnungslos ineffizient! Die konkreten Daten und Problemstellungen ändern sich ständig, daher benötigen wir allgemeine Methoden, die möglichst universell einsetzbar sind. Dieser Werkzeugkasten erlaubt effizientes Arbeiten.
- Abstraktion hilft und vereinfacht! Die Mathematik versucht, Ergebnisse zu bündeln, Muster zu erkennen, Gemeinsamkeiten zu nutzen, und so eine möglichst universelle Beschreibung von Problemen und Lösungen bereitzustellen.

Wie können wir sicher sein, dass neu gefundene Ergebnisse korrekt sind, also Sätze, Methoden, Algorithmen, ... wirklich leisten, was sie versprechen? Natürlich können wir eine allgemeine Aussage anhand von konkreten Beispielen testen, und so eventuell Fehler finden. Leider genügen noch so viele erfolgreiche Beispiele noch nicht, um zu garantieren, dass die Aussage wirklich immer gilt. Anders als andere Wissenschaften besitzt die Mathematik hierzu eine Geheimwaffe: den **Beweis**!

Um als Satz zu gelten, muss die behauptete Aussage bewiesen werden. Andernfalls ist sie bloß eine Vermutung und sollte ehrlicherweise auch so genannt werden. Auf diese Weise hat jede wichtige Aussage einen unmissverständlichen Status: Sie ist entweder bewiesen, widerlegt oder noch offen.

Einordnung in das Mathematikstudium. Ab dem ersten Studienjahr lernen Sie in den Vorlesungen **Lineare Algebra** und **Analysis**, wie Sie einen Beweis richtig ausführen. Dazu benötigen Sie viel Übung und Erfahrung und Kenntnis erfolgreicher Beweismethoden, wie zum Beispiel den direkten Beweis durch Konstruktion (wie oben gesehen), den indirekten Beweis durch Widerspruch, die Kontraposition, die Fallunterscheidung, den Beweis durch Ringschluss, die vollständige Induktion und für Hartgesottene sogar die transfinite Induktion. Wenn Sie diese bewährten Techniken kennen, dann fällt Ihnen das Beweisen viel leichter. Das Ziel sind zwei sich ergänzende Fähigkeiten:

- Lesen: einen vorgelegten Beweis detailliert nachvollziehen und kritisch prüfen
- Schreiben: einen neuen Beweis selbst finden und korrekt ausführen

Im ersten Semester beginnen Sie dazu mit der **Logik**, aus der Sie alle nötigen Beweismethoden ableiten können. Sie lernen dabei, logisch schlüssig zu argumentieren, Behauptungen und Beweise genau zu formulieren, typische Fehler und Trugschlüsse zu vermeiden. Sie beginnen mit den einfachen Grundlagen: Implikationen oder Äquivalenzen zeigen; zusammengesetzte Aussagen richtig negieren; Aussagen widerlegen, etwa durch ein Gegenbeispiel.

Stufe 3 / Phantastisch große Primzahlen und wozu sie nützlich sind.

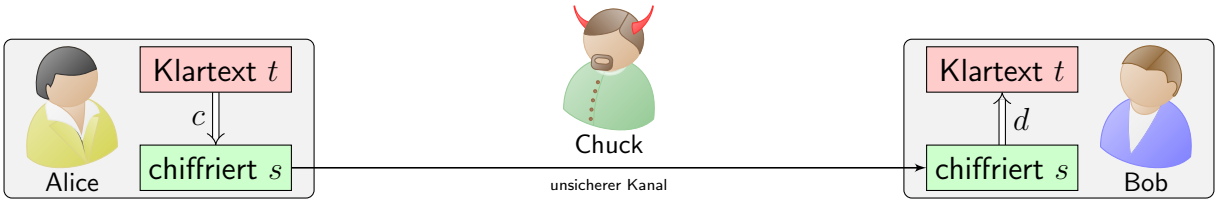
Primzahlen sind seit Jahrhunderten ein faszinierendes Forschungsobjekt der Mathematik, seit Jahrzehnten finden Sie zudem zahlreiche Anwendungen in der Informatik, besonders der Kryptographie.

Der oben angegebene Beweis ist **konstruktiv**, er beschreibt ein explizites Verfahren, mit dem wir beliebig viele Primzahlen **konstruieren** können: „Gib mir eine endliche Liste $(p_1, p_2, \ldots, p_n)$ von Primzahlen, und ich berechne dir daraus eine weitere Primzahl." Hierzu ein konkretes Beispiel:

- Wir starten mit der Primzahl 5, also der einelementigen Liste (5), berechnen die Primzerlegung von $q = 6$ zu $q = 2 \cdot 3$ und erhalten so die neuen Primzahlen 2 und 3.
- Wir beginnen erneut mit der Liste $(2, 3, 5)$, berechnen die Primzerlegung von $q = 31$ und erhalten die neue Primzahl 31.
- Wir iterieren das Verfahren für $(2, 3, 5, 31)$, berechnen die Primzerlegung von $q = 931$ zu $q = 7 \cdot 7 \cdot 19$ und erhalten so die neuen Primzahlen 7 und 19.

Mit dieser Methode erhalten wir in jedem Schritt mindestens eine neue Primzahl: Das haben wir bewiesen! So können wir beliebig viele konstruieren, vorausgesetzt wir haben beliebig viel Zeit... Unser Algorithmus ist für große Primzahlen nicht effizient, sondern sehr zeitaufwändig. Es ist recht leicht, die Zahl $q = p_1 \cdot p_2 \cdots p_n + 1$ auszurechnen, hingegen ist die Primzerlegung sehr rechenintensiv. Hierzu ist bislang kein ausreichend schnelles Verfahren bekannt!

Die Multiplikation ist leicht, aber die Zerlegung ist schwer. Diesen Fluch können wir auch als Segen betrachten: Die **Kryptographie** nutzt dies geschickt, um Daten sicher zu verschlüsseln. Das **RSA–Kryptosystem** ist das erste *asymmetrische* Verschlüsselungsverfahren und bis heute weit verbreitet. Entwickelt wurde es 1977 von R. Rivest, A. Shamir und L. Adleman, siehe `en.wikipedia.org/wiki/RSA_(cryptosystem)`. Wir fassen die Kernidee hier schematisch zusammen.



Zur **Herstellung** seines Schlüsselsatzes benötigt Bob zwei große Primzahlen p und q, sagen wir jede mit etwa 600 Dezimalstellen. Dafür gibt es schnelle Verfahren. Daraus berechnet Bob das Produkt $n = pq$ sowie $m = (p-1)(q-1)$. Zudem wählt er $c, d \in \mathbb{N}$, sodass $cd = 1$ modulo m gilt. Das Rechnen mit Restklassen erklären wir in unserer Beispielaufgabe „Rekursion und Prüfziffer".

Bobs vollständiger Schlüssel ist (n, c, d). Die Primzahlen p, q werden im Folgenden nicht mehr benötigt. Der Schlüssel (n, c, d) wird nun in einen öffentlichen (n, c) und einen privaten Teil (n, d) aufgeteilt. Bob veröffentlicht (n, c) und behält (n, d) sorgsam für sich allein.

$$\begin{array}{llll} \text{Öffentlicher Schlüssel } (n,c) & - & \text{Verschlüsselung} & \mathbb{Z}/n \to \mathbb{Z}/n \,:\, t \mapsto s = t^c \\ \text{Privater Schlüssel } \quad (n,d) & - & \text{Entschlüsselung} & \mathbb{Z}/n \to \mathbb{Z}/n \,:\, s \mapsto t = s^d \end{array}$$

Alice möchte Bob eine Nachricht $t \in \mathbb{Z}/n$ schicken. Sie berechnet dazu die verschlüsselte Botschaft $s = t^c$. Diese schickt sie an Bob, und dieser berechnet daraus wieder den Klartext $s^d = t$. Voilà!

Korrektheit: Ver- und Entschlüsselung sind zueinander invers: Für alle $t \in \mathbb{Z}/n$ gilt $(t^c)^d = t^{cd} = t$. Das ist ein grundlegender Satz, sein Beweis garantiert die Korrektheit des RSA–Kryptosystems.

Sicherheit: Allein mit Kenntnis von n, c, s lässt sich der Klartext $t = s^d$ nur mit „unwirtschaftlich hohem Aufwand" berechnen. Das ist eine Vermutung, die bisher weder bewiesen noch widerlegt ist.

Chuck hat eine offensichtliche Angriffsmöglichkeit: Finde die Primzerlegung $n = pq$, berechne daraus $m = (p-1)(q-1)$ und schließlich d. Für große Primzahlen p, q scheitert das an der Primzerlegung.