Universität Stuttgart

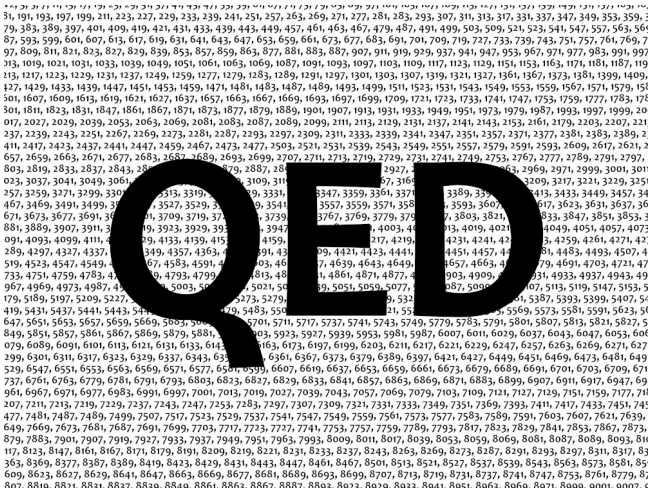
Beispielaufgabe zur Studienwahl

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 $q = p + 1 \geq 2$.	☐

Weitere Aufgaben und Informationen unter:
Studienwahl-Kompass Mathematik
Universität Stuttgart

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 keine Fehler enthält und keine 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.

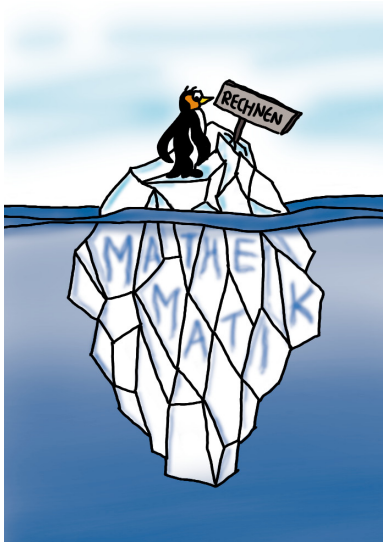
Wie bringen wir jetzt die Schritte (3)–(6) in die richtige Reihenfolge? Einfache Grundregel: Alle Bezeichnungen und Variablen, die wir verwenden, müssen wir zuvor einführen und erklären. Hier bedeutet das konkret: Aussage (6) fasst zusammen, was in (5) ausgeführt wurde. Schritt (5) benötigt Schritt (4), 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.

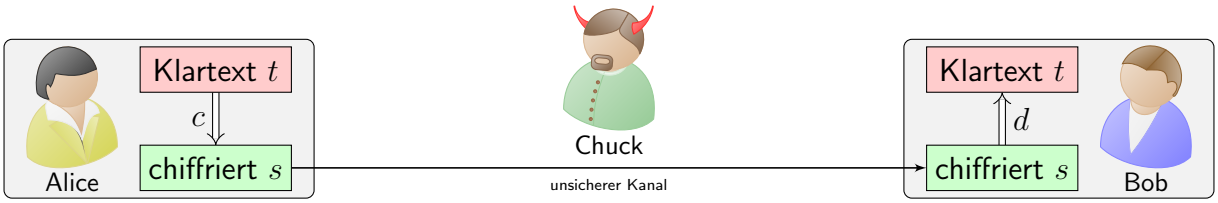
Primzahlen sind seit Jahrhunderten ein faszinierendes Forschungsobjekt der Mathematik, seit Jahrzehnten finden Sie zudem zahlreiche Anwendungen in der Informatik, besonders der Kryptographie.

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.

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

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.