„Straßenkampfmathematik“
und andere Ansätze der Ingenieursmathematik

Jens-Peter M. Zemke
zemke@tu-harburg.de

Institut für Numerische Simulation
Technische Universität Hamburg-Harburg

19.10.2010

TUHH
Technische Universität Hamburg-Harburg

Übersicht

Hintergrund zum Vortrag

Straßenkampfmathematik
- Dimensionsanalyse
- Einfache Fälle
- Klumpenbildung
- Bildhafte Beweise
- Das Wichtigste zuerst
- Analogie

Wie man rechnet

Auswahl der „schönsten“ Berechnung
- Unendlich viele Primzahlen: Euklids Beweis
- Unendlich viele Primzahlen: Eulers Beweis
- Fundamentalsatz der Algebra: Argands Beweis

Wenn alles andere versagt . . .

Hintergrund

Die an einer Technischen Universität verwendete Mathematik unterscheidet sich von Schulmathematik:

- Man sollte besser nicht zu viel rechnen. Das ist der Ansatz im Buch “Street-Fighting Mathematics”, erschienen am MIT unter einer Creative Commons (CC) Lizenz, genauer CC-BY-NC-SA, (Mahajan, 2010).
- Da man manchmal doch rechnen muss, sollte man wissen, ob und wie. Das findet man in den Büchern “How to solve it” (Polya, 2004), “Dead reckoning” (Doerfler, 1993) und “How to calculate quickly” (Sticker, 2000).
- Wenn man sich die Rechnung aussuchen kann, sollte man einen „schönen“ Weg aussuchen. Dazu: “Proofs from the book” (Euklid, Euler), nach (Aigner and Ziegler, 1999), und der Fundamentalsatz der Algebra (Argand) nach (Königsberger, 2004, §7.6).
- Manchmal geht es nicht „schön“ und man nimmt, was man kriegt. Ein Beispiel dazu ist der Satz „Alle endlichen Gruppen ungerader Ordnung sind auflösbar“, bewiesen von Walter Feit und John Griggs Thompson (Feit and Thompson, 1963) (hier nur im Ansatz gezeigt).

Motivation

Man kann Aufgaben mit mathematischem Hintergrund oft auf zwei verschiedene Arten stellen:

> *„Ein Ball falle aus Ruhelage aus einer Höhe von h Metern und berühre den Boden mit einer Geschwindigkeit von v Metern pro Sekunde. Berechnen Sie v unter der Annahme einer gravitionellen Beschleunigung von g Metern pro Sekunde zum Quadrat und unter Vernachlässigung des Luftwiderstandes.“*

> *„Ein Ball falle aus Ruhelage aus einer Höhe von h und berühre den Boden mit einer Geschwindigkeit von v. Berechnen Sie v unter der Annahme einer gravitionellen Beschleunigung von g und unter Vernachlässigung des Luftwiderstandes.“*

Welcher Ansatz hat welche Vor- und Nachteile?

Vergleich anhand der Lösung

Die erste Aufgabenstellung ist einheiten- und dimensionslos gestellt. Die Einheiten sind explizit vorgegeben. Die zweite Aufgabenstellung bietet die Freiheit/Pflicht, selber Einheiten zu überlegen.

Dafür hat man bei der zweiten Aufgabenstellung eine Kontrolle des Ergebnisses: Es bezeichne x die Höhe über dem Boden und t die Zeit, sowie v die Geschwindigkeit und a die Beschleunigung. Dann ist

$$x(0) = h, \quad v = \frac{dx}{dt} = \dot{x}, \quad v(0) = 0, \quad a = \frac{dv}{dt} = \frac{d^2x}{dt^2} = \ddot{x} = -g = \text{const.} \tag{1}$$

und es gilt

$$x(t) = -\frac{1}{2}gt^2 + h. \tag{2}$$

Die Endschnelligkeit (bei $x = 0$, also $t = \sqrt{2h/g}$) beträgt demnach

$$|v(\sqrt{2h/g})| = |-g\sqrt{2h/g}| = \sqrt{2gh}. \tag{3}$$

Dimensionsanalyse

Man sieht, dass $\sqrt{2gh}$ die korrekte Dimension einer Geschwindigkeit hat, nämlich $\dim(\sqrt{2gh}) = \sqrt{L/T^2 \cdot L} = L/T$.

Andersherum: Um eine Geschwindigkeit aus g und h zu kombinieren, also die Dimension L/T, muss die Abhängigkeit von g als einzig zeitabhängigem Anteil in der Form $\sqrt{g}$ vorliegen. Damit muss der fehlende Anteil $\sqrt{L}$ von $\sqrt{h}$ kommen, also wissen wir ohne Rechnung

$$v \sim \sqrt{gh}, \tag{4}$$

wobei

$$a \propto b \quad :\Leftrightarrow \quad a \text{ und } b \text{ haben (evtl. dimensionsabhängigen) Faktor,} \tag{5a}$$
$$a \sim b \quad :\Leftrightarrow \quad a \text{ und } b \text{ haben dimensionsunabhängen Faktor,} \tag{5b}$$
$$a \approx b \quad :\Leftrightarrow \quad a \text{ und } b \text{ haben Faktor nahe Eins.} \tag{5c}$$

Es fehlt also zum Endergebnis nur der dimensionslose Faktor $\sqrt{2}$.

Dimensionsanalyse

Was nützen die obigen Überlegungen bei der Berechnung des Integrales

$$\int_{-\infty}^{\infty} e^{-5x^2} dx? \tag{6}$$

Zuerst verallgemeinert man die Fragestellung: Welchen Wert hat

$$\int_{-\infty}^{\infty} e^{-\alpha x^2} dx? \tag{7}$$

Das Ergebnis hängt nicht mehr von x ab, es gibt auch keine Integrationskonstante. Das Ergebnis ist eine Funktion alleine von α,

$$\int_{-\infty}^{\infty} e^{-\alpha x^2} dx = f(\alpha). \tag{8}$$

Dimensionsanalyse

Wir versehen jetzt x und α mit Dimensionen, so dass die Gleichung erfüllt ist. Dadurch gewinnen wir Aufschluss über die möglichen Funktionen $f(\alpha)$: Der Plan lautet

- versehe α mit Dimensionen,
- finde die Dimensionen des Integrales,
- bastele ein $f(\alpha)$ mit diesen Dimensionen.

Die Variable x hat in natürlicher Weise die Dimension einer Länge, $[x] = L$: Es wird über die x-Achse integriert.

Die Variable α erscheint im Exponenten, zusammen mit x. Exponenten geben an, „wie oft“ eine Zahl mit sich selbst multipliziert wird, ist also dimensionslos. Damit muss $[\alpha][x]^2 = 1$ gelten, α also die Dimension $[\alpha] = L^{-2}$ haben.

Dimensionsanalyse

Der Exponentialterm ist also dimensionslos. Das Integral ist (z. B.) als Verfeinerung einer Treppenfunktion definiert, im Limes hat also $\Delta x \to dx$ die selbe Dimension wie x, also ist $[dx] = L$ und das Ergebnis der Integration ist eine Länge.

Damit muss aber die Funktion $f(\alpha)$ auch die Dimension einer Länge haben,

$$L = \left[\int_{-\infty}^{\infty} e^{-\alpha x^2} dx\right] = [f(\alpha)]. \tag{9}$$

Eine kurze Überlegung zeigt, dass dann

$$f(\alpha) \sim \frac{1}{\sqrt{\alpha}} \tag{10}$$

gelten muss, also für eine unbekannte Konstante c

$$\int_{-\infty}^{\infty} e^{-\alpha x^2} dx = \frac{c}{\sqrt{\alpha}}. \tag{11}$$

Zurück zum Integral

Wir betrachten nochmals das Integral

$$\int_{-\infty}^{\infty} e^{-\alpha x^2} dx. \tag{12}$$

Eine typische Studentenfrage lautet: War das Ergebnis nun $\sqrt{\pi\alpha}$ oder $\sqrt{\pi/\alpha}$? (Wer Dimensionsanalyse kann, sieht es sofort.)

Um solche Fragen beantworten zu können, sucht man nach einfachen (Spezial-)Fällen.

- Für $\alpha \to \infty$ geht die Fläche unter der Funktion gegen Null, da die Glockenkurve immer steiler wird.
- Für $\alpha \to 0$ konvergiert die Funktion gegen die konstante Funktion $e^0 = 1$, das Integral sollte also gegen ∞ divergieren.
- Für $\alpha = 1$ verwendet man eine Formel zur approximativen Integration, eine sogenannte Quadraturformel. Man sieht dann schnell, dass das Integral einen Wert nahe bei $\sqrt{\pi} \approx 1.772453850905516$ annimmt.

„π mal Daumen“

Oft muss eine Integration durchgeführt werden, welche durch eine Flächenberechnung veranschaulicht werden kann.

Wir betrachten allgemeine Zerfallsprozesse. Diese werden durch Funktionen $e^{-\alpha t}$ mit $\alpha > 0$ beschrieben. Das zugehörige Integral

$$\int_0^\infty e^{-\alpha t} dt \tag{13}$$

„klumpt“ eigentlich nur nahe Null, daher ersetzt man die Fläche unter der Funktion durch ein Rechteck mit der Höhe gleich dem Maximum der Funktion, hier, $1 = e^0 = \max_{x \in (-\infty, 0]} e^x$.

Als Breite des Rechteckes wählt man entweder die „$1/e$“-Heuristik oder die Volle-Breite-bei-halbem-Maximum–Heuristik (VBhM).

„$1/e$“-Heuristik

Die „$1/e$“-Heuristik nimmt als Breite des Rechteckes den Wert $t \in [0, \infty)$, an dem die Funktion $e^{-\alpha t}$ gleich der für die Exponentialfunktion „signifikanten Änderung“ $1/e$ ist, also $t = 1/\alpha$.

Diese „signifikante Änderung“ ist motiviert aus der Beobachtung, dass e^{-2} z. B. bedeutet, dass man den Ausgangswert $1 = e^0$ zweimal durch e teilt. Bei solchem wiederholtem Teilen durch e ist ein einmaliges Teilen sicherlich signifikant.

Damit ergibt sich als „geklumpter“ Wert des Integrales

$$\int_0^\infty e^{-\alpha t} dt \approx e^0 \cdot \frac{1}{\alpha} = \frac{1}{\alpha}. \tag{14}$$

Dieser Wert ist aber sogar der korrekte Wert, wie man nach der Substitution $x = -\alpha t$ durch nachfolgende Antiderivation schnell berechnen kann.

„$1/e$“-Heuristik und etwas Stochastik

Die „$1/e$“-Heuristik kann man sich auch anders überlegen: Betrachtet als Wahrscheinlichkeitsdichtefunktion (nach Skalierung), liegt der Erwartungswert der Funktion $e^{-\alpha t}$ auf $[0, \infty)$ bei $1/\alpha$.

Erklärungen dazu: Eine Dichtefunktion f dient dazu, für stetige Verteilungen die Wahrscheinlichkeit zu beschreiben, dass ein Ereignis zwischen $a < b$ eintritt,

$$P(a \leqslant x \leqslant b) = \int_a^b f(x)dx. \tag{15}$$

Der Erwartungswert ist dann wie im analogen Fall einer diskreten Wahrscheinlichkeitsverteilung gegeben als

$$E(T) = \int_{-\infty}^{\infty} tf(t)dt. \tag{16}$$

Dazu muss man aber wieder die zu integrierende Funktion (nach partieller Integration) integrieren . . .

VBhM-Heuristik

Die Volle-Breite-bei-halbem-Maximum–Heuristik funktioniert gut, wenn der zu viel gezählte und der weggelassene Flächenteil gleich groß ist. Hier ergibt sich die Breite aus

$$e^{-\alpha t} = \frac{1}{2} = \frac{e^0}{2} \tag{17}$$

zu $t = \ln(2)/\alpha$, und damit die approximative Fläche unter dem Integral zu

$$\int_0^\infty e^{-\alpha t} dt \approx e^0 \cdot \frac{\ln(2)}{\alpha} = \frac{\ln(2)}{\alpha} \approx \frac{0.69315}{\alpha}. \tag{18}$$

Damit ist der absolute Fehler bei dieser „Klumpenbildung“ ungefähr $(3\alpha)^{-1}$.

In diesem einfachen Fall ist die „$1/e$-Heuristik“ der klare Gewinner. Beide Heuristiken entsprechen sogenannten Quadraturformeln, die man im allgemeinen Fall vergleichen kann, und bei diesem Vergleich schneidet die VBhM-Heuristik besser ab.

Vergleich am Beispiel

Wir vergleichen die beiden Heuristiken am Beispiel

$$\int_{-\infty}^{\infty} e^{-\alpha x^2} dx = 2 \int_{0}^{\infty} e^{-\alpha x^2} dx. \tag{19}$$

Für die „$1/e$-Heuristik“ ist die Breite durch

$$e^{-\alpha x^2} = e^{-1} \tag{20}$$

zu $x = \sqrt{1/\alpha}$ festgelegt, der approximative Wert des Integrales ist demnach

$$\int_{-\infty}^{\infty} e^{-\alpha x^2} dx \approx \frac{2 \cdot 1 \cdot 1}{\sqrt{\alpha}}. \tag{21}$$

Dieses ist für den geringen Rechenaufwand ein gutes Ergebnis nahe am wirklichen Wert

$$\int_{-\infty}^{\infty} e^{-\alpha x^2} dx = \sqrt{\frac{\pi}{\alpha}} \approx \frac{1.77}{\sqrt{\alpha}}. \tag{22}$$

Vergleich am Beispiel

Die VBhM-Heuristik erzwingt die Breite nach

$$e^{-\alpha x^2} = \frac{1}{2}, \tag{23}$$

also als $x = \sqrt{\ln(2)/\alpha}$.

Damit ist das approximative Ergebnis nach dieser Heuristik gegeben durch

$$\int_{-\infty}^{\infty} e^{-\alpha x^2} dx \approx \frac{2 \cdot \sqrt{\ln(2)}}{\sqrt{\alpha}} \approx \frac{1.66510922}{\sqrt{\alpha}}. \tag{24}$$

Der absolute Fehler für die beiden Heuristiken passt in das oben behauptete allgemeine Verhalten:

$$\text{absoluter Fehler bei } 1/e \approx \frac{0.2275461}{\sqrt{\alpha}}, \tag{25}$$

$$\text{absoluter Fehler bei VBhM} \approx \frac{0.1073446}{\sqrt{\alpha}}. \tag{26}$$

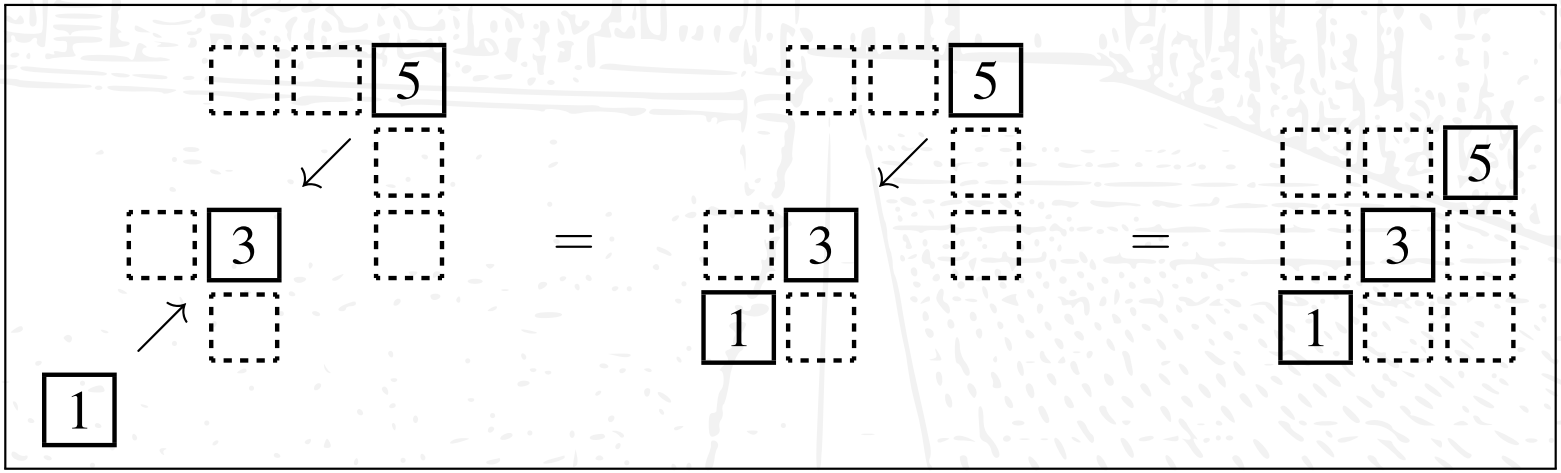
Ein Bild sagt mehr als tausend Worte . . .

Manchmal ist es einfacher, ein Bild zu verwenden, als viele mathematische Formeln „runterzurattern“.

Als Einführung: Man vermutet schnell, dass die Summe der ersten k ungeraden natürlichen Zahlen die Quadratzahl k^2 ergibt:

$$1 = 1^2, \quad 1+3 = 2^2, \quad 1+3+5 = 3^2, \quad 1+3+5+7 = 4^2, \quad \ldots \tag{27}$$

Häufig wird dieser Sachverhalt mittels vollständiger Induktion bewiesen. Dabei ist der skizzierte bildhafte Beweis „anschaulicher“ (sic) und somit leichter zu verstehen (und leichter zu merken):

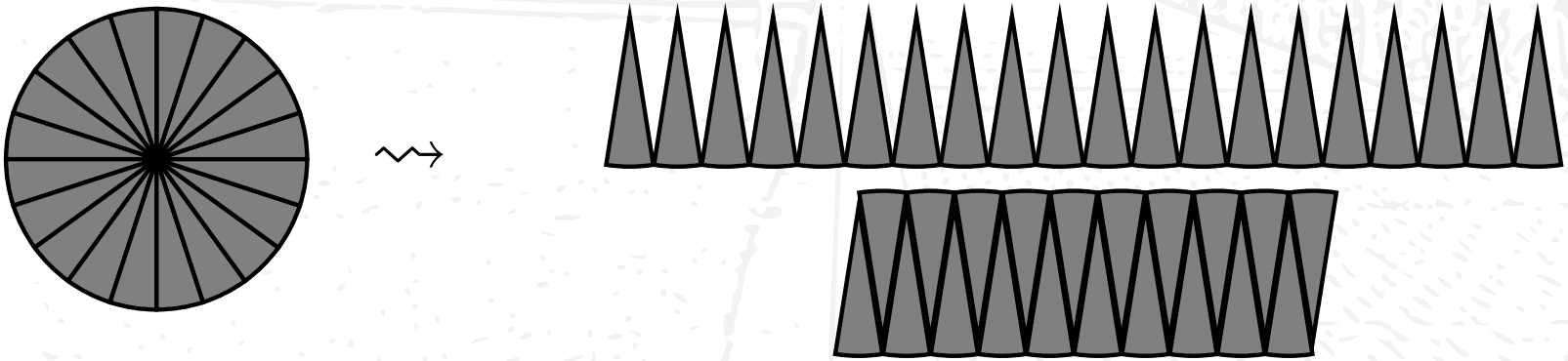


Die Sache mit π

Die Griechen fanden schnell heraus, dass alle Kreise ein festes Verhältnis zwischen Diameter (Zwei mal Radius) und Kreisumfang aufweisen. Dieses nannten sie π (eigentlich nicht). Es gilt also für den Umfang U eines Kreises mit Radius r und Diameter $d = 2r$ die Gleichung

$$U = \pi d = 2\pi r. \tag{28}$$

Auch den Griechen war (Dimensionsanalyse!) schon klar, dass es eine Konstante geben müsse, die dasselbe für den Flächeninhalt F geteilt durch den Radius zum Quadrat erfüllt. Sie zeigten mittels des folgenden bildhaften Beweises, dass auch diese Zahl gleich π ist, also $F = \pi r^2$ gilt:



Welches Mittel denn nun?

Es gibt verschiedene Arten der Mittelbildung, darunter das arithmetische und das geometrische Mittel. Seien $a \geqslant b \geqslant 0$ zwei reelle Zahlen. Dann ist das arithmetische Mittel definiert durch

$$AM = \frac{a+b}{2}, \tag{29}$$

das geometrische Mittel hingegen ist definiert durch

$$GM = \sqrt{a \cdot b}. \tag{30}$$

Man kann schnell beweisen, dass das arithmetische Mittel immer größer oder gleich dem geometrischen Mittel ist, also $AM \geqslant GM$, allerdings ist der Standardbeweis nicht unbedingt offensichtlich.

Welches Mittel denn nun?

Wir geben kurz den Standardbeweis an. Offensichtlich ist $(a-b)^2 \geqslant 0$. Also gilt (man beachte $a, b \geqslant 0$)

$$(a-b)^2 = a^2 - 2ab + b^2 \geqslant 0 \tag{31a}$$

$$\Leftrightarrow \quad a^2 + 2ab + b^2 \geqslant 4ab \tag{31b}$$

$$\Leftrightarrow \quad (a+b)^2 \geqslant 2^2 ab \tag{31c}$$

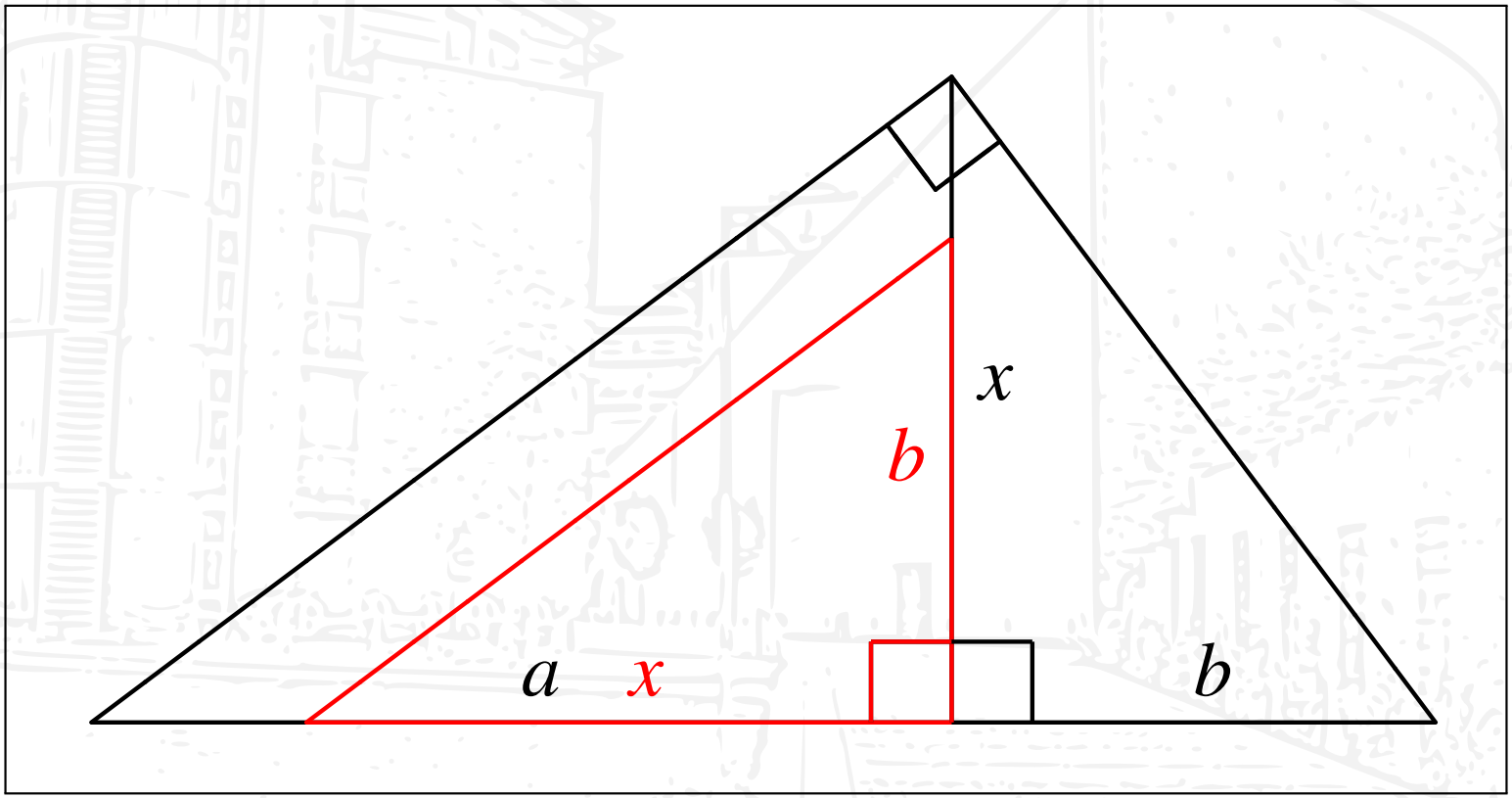
$$\Leftrightarrow \quad a + b \geqslant 2\sqrt{ab} \tag{31d}$$

$$\Leftrightarrow \quad AM = \frac{a+b}{2} \geqslant \sqrt{ab} = GM. \tag{31e}$$

Der Beweis ist sicherlich elegant, aber woher weiß man, dass man mit $(a-b)^2$ starten soll? Warum addiert man auf einmal $4ab$ zu beiden Seiten der Ungleichung? Klar, weil es funktioniert. Aber klärt das das „Warum“?

“the kind of gestalt insight”

Man kann folgendes Dreieck konstruieren:



Man sieht schnell, dass $x = \sqrt{ab}$, da aufgrund der Ähnlichkeit der Dreiecke $a/x = x/b$ gilt. Das geometrische Mittel ist also die Höhe des konstruierten rechtwinkligen Dreiecks.

“the kind of gestalt insight”

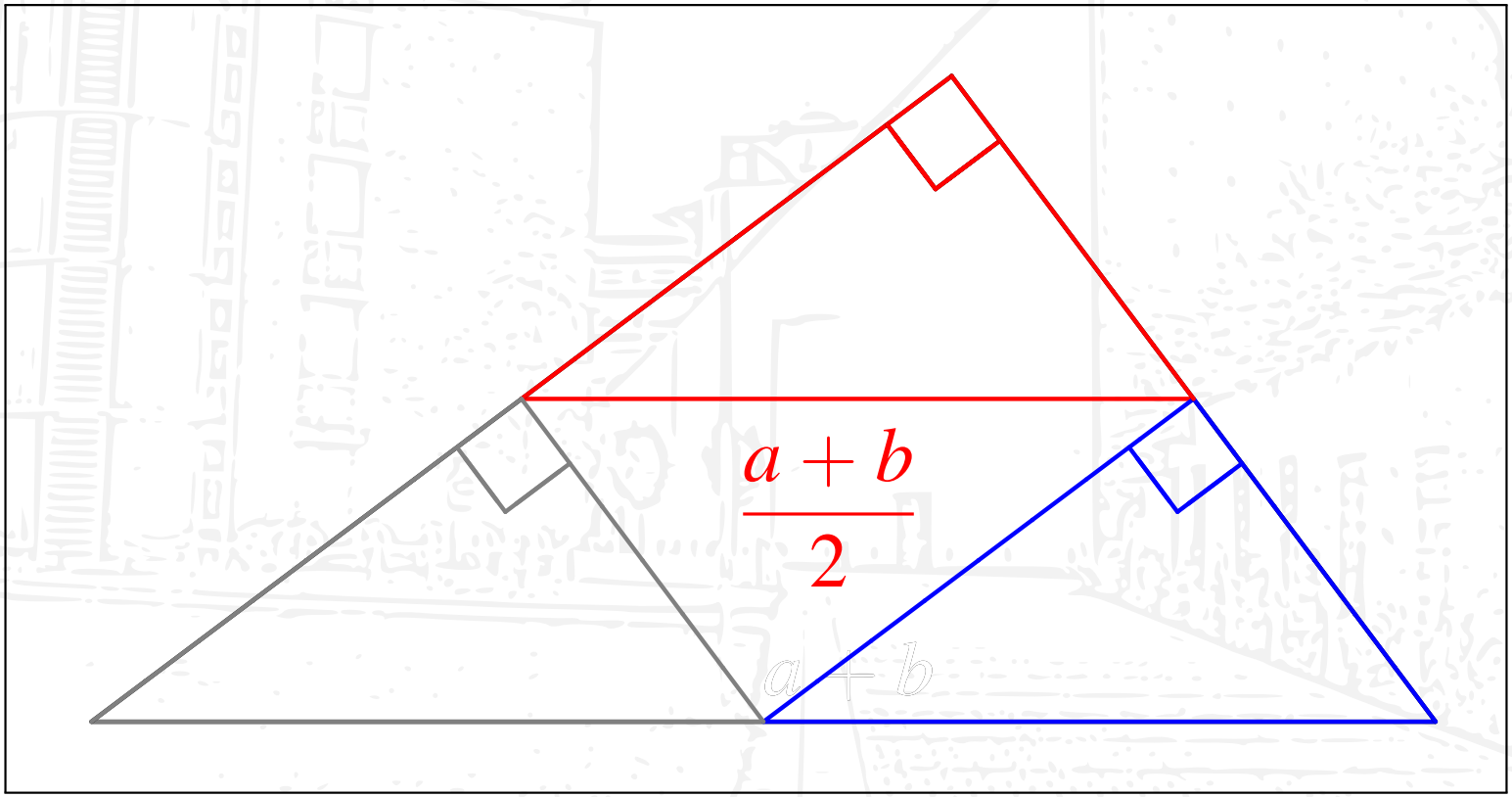
Man kann zu jedem Dreieck einen Kreis finden, der alle drei Ecken des Dreieckes berührt.

Der Beweis arbeitet wieder graphisch: Man kann sich den Mittelpunkt einer Dreiecksseite als Mittelpunkt und als Radius die halbe Seitenlänge aussuchen. Dann berührt dieser Kreis zumindest zwei Eckpunkte, generell aber nicht den dritten.

Nun kann man entlang einer senkrecht zur gewählten Seite stehenden Geraden durch den Mittelpunkt den Kreismittelpunkt verschieben und den Radius so wählen, dass immer noch die zwei Ecken berührt werden. Durch Wahl dieser Verschiebung kann man sicherstellen, dass alle drei Ecken berührt werden.

“the kind of gestalt insight”

Das Auffinden dieses Kreises ist hier aber sehr einfach: Man betrachte das folgende Bild.



Klarerweise ist der Radius des einhüllenden Kreises größer oder gleich der Höhe des Dreiecks. Damit ist aber $AM \geqslant GM$.

Datenkapazität einer CD

Eine Compact-Disc (CD) kann

$$\underbrace{1\,h \times \frac{3600\,s}{1\,h}}_{\textit{Abspielzeit}} \times \underbrace{\frac{4.4 \times 10^4\,\text{samples}}{1\,s}}_{\textit{Samplerate}} \times \underbrace{2\,\text{Kanäle} \times \frac{16\,\text{bits}}{1\,\text{sample}}}_{\textit{Samplegröße}} \tag{32}$$

an (Audio-)Daten aufnehmen.

Das sind ungefähr jeweils 3, 4 und eine Potenz(en) von 10, also befinden wir uns in der Größenordnung von 10^8 bits. Damit haben wir die Zehnerpotenz an bits bereits geschätzt.

Um genauer zu werden, betrachtet man jetzt die Vorfaktoren, also

$$3.6 \times 4.4 \times 3.2. \tag{33}$$

Datenkapazität einer CD

In solchen Produkten ersetzt man die gegebenen Zahlen durch eines der drei Elemente 1, „wenige“ oder 10. Wie groß sollte man „wenige“ wählen?

Da man mit einer Multiplikation arbeitet, bietet sich das geometrische Mittel zwischen 1 und 10, also $\sqrt{10} \approx 3$ an. Sei also „wenige“ gegeben durch $\sqrt{10}$ und manchmal weiter abgeschätzt durch 3.

Dann gilt

$$3.6 \times 4.4 \times 3.2 \approx (\text{„wenige“})^3 \approx 30. \tag{34}$$

Damit ist die Kapazität geschätzt durch 3×10^9 bits.

Die wirkliche Kapazität liegt übrigens bei 5.6×10^9 bits.

Die Einteilung von Zahlen in 1, „wenige“ und 10 bietet sich oft an und ist recht hilfreich, auch wenn „wenige“ eigentlich nie genau gegeben ist.

Topologie

Wir betrachten den Ansatz der Analogie anhand der folgenden topologischen Fragestellung:

> *In wieviele Regionen wird der Raum zerlegt, wenn man fünf Ebenen hindurchlegt?*

Zuerst wird man nach einfachen Fällen suchen: Null Ebenen zerlegen den Raum in eine Region (also gar nicht), eine Ebene zerlegt den Raum in zwei Regionen, drei Ebenen schneiden im allgemeinen Fall wieder die beiden so erhaltenen Regionen entzwei, also erhalten wir $4 = 2 \cdot 2$ Regionen, erneutes Schneiden liefert $8 = 2 \cdot 4$ Regionen.

Wir erhalten so die folgende Tabelle für die Anzahl $R(n)$ der Regionen:

n	0	1	2	3	4	5
$R(n)$	1	2	4	8	16	32

(35)

Das Muster legt den Verdacht nahe, dass $R(n) = 2^n$ gilt.

Topologie

Um voranzukommen, betrachtet man jetzt dieselbe Fragestellung in niederer Dimension, nämlich der Ebene statt im Raum, als Schnitte dienen dabei Geraden statt Ebenen. Als Erwartungshaltung könnte man das Bildungsgesetz $R(n) = 2^n$ im Hinterkopf haben.

Keine Gerade schneidet eine Ebene gar nicht, eine Gerade schneidet eine Ebene in zwei Teile, die nächste Gerade schneidet die beiden Teile in insgesamt $4 = 2 \cdot 2$ Teile. Jippie!

Es ist aber jetzt durch keine Wahl der nächsten Schnittgeraden möglich, alle Regionen wieder zu zerteilen. Man schafft maximal drei der vier Regionen, also gilt $R(3) = 7 \neq 8 = 2^3$. Die nächste Schnittgerade kann dann maximal vier Regionen teilen, also gilt $R(4) = 11$.

Damit ist das Muster (Pattern) $R(n) = 2^n$ in der Ebene falsch, was auch nicht gerade Hoffnung macht für die Ausgangsfragestellung.

Topologie

Jetzt betrachtet man auch noch den Fall einer Geraden, welche durch n Punkte in Regionen (Segmente) zerlegt wird.

Nein, es sind nicht n Segmente bei n Punkten . . . :-)

. . . sondern, wie der Fall eines Punktes nahelegt, $n+1$ Segmente.

Damit haben wir für die Gerade, Ebene und den Raum die folgende Tabelle:

n	0	1	2	3	4	5	n
$R_1(n)$	1	2	3	4	5	6	$n+1$
$R_2(n)$	1	2	4	7	11		
$R_3(n)$	1	2	4	8			

(36)

Man erkennt aber neue Muster nach längerem Hinschauen:

- $R_d(n) = 2^n$ für $n \leqslant d$,
- $R_d(n) = R_{d-1}(n-1) + R_d(n-1)$.

Topologie

Zum Glück sind beide Vermutungen korrekt, also ist die gesuchte maximale Anzahl der Regionen, in die fünf Ebenen den Raum zerteilen, gegeben durch

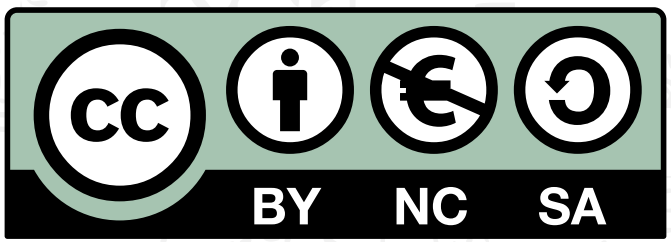
$$\begin{aligned} R_3(5) &= R_2(4) + R_3(4) \\ &= 11 + R_2(3) + R_3(3) \\ &= 11 + 7 + 8 \\ &= 11 + 15 = 26. \end{aligned} \tag{37}$$

Dieselbe Antwort erhält man auch durch „brute force“, also durch sich fünf Ebenen im Raum vorstellen . . . aber der soeben vorgestellte Ansatz zeigt noch mehr auf: Man kann rückschließen, dass $R_0(n) = 1$ eine konsistente Definition ist, man kann sehen, dass dieses ein konstantes Polynom in n ist, dass $R_1(n) = n + 1$ ein lineares Polynom in n ist, und vermuten, dass $R_2(n)$ ein quadratisches und $R_3(n)$ ein kubisches Polynom in n ist.

Topologie

Im Buch “Street-Fighting Mathematics”, (Mahajan, 2010), geht Sanjoy Mahajan noch weiter mit diesem Beispiel für Analogie. Der bisherige Teil der OE-Vorlesung basiert auf diesem Buch. Da das Buch recht lesenswert ist, und unter einer CC-Lizenz steht, sei es jedem Erstsemester ans Herz gelegt.

Diese Folien sind in Analogie zum Buch von Sanjoy Mahajan auch unter



“Dead Reckoning”

Manchmal ergibt es sich, dass man doch rechnen muss. Das Buch “Dead Reckoning” (eigentlich „Koppelnavigation“, gemeint als „totes Rechnen“, ergo, ohne Hilfsmittel) von Ronald W. Doerfler bietet viele Tricks dazu.

Schnelles oder vereinfachtes Rechnen mit ganzen Zahlen basiert meist auf zwei Dingen:

- Wir rechnen im Zehnersystem,
- Es fällt leichter, mit Zweier- oder Dreiergruppen von Ziffern zu rechnen.

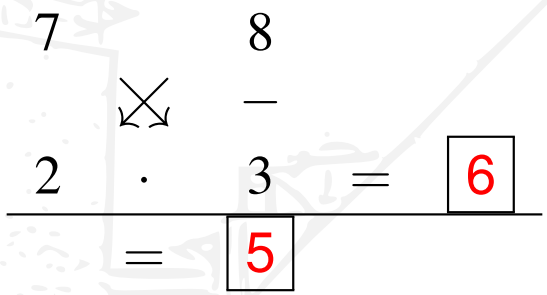
Die erste Beobachtung sagt uns zum Beispiel, dass eine Multiplikation mit einer Zehnerpotenz nur ein Verschieben um eine entsprechende Stellenzahl der Ziffern bewirkt,

$$223 \cdot 100 = 22300. \tag{38}$$

Der leichtere Umgang mit Zweier- oder Dreiergruppen kommt vom Rechnen mit Geld (Cent-Beträge sind zweistellig) und von der von uns verwendeten Notation (Eins, Tausend, Million, Milliarde, . . .).

“Dead Reckoning”

Hier ein Beispiel zur Multiplikation zweier ganzer Zahlen: Um etwa den Wert von $7 \cdot 8$ zu berechnen, verwendet man die folgende Rechenvorschrift:



(39)

Damit haben wir die beiden Ziffern von $56 = 7 \cdot 8$ berechnet.

Was auf den ersten Blick wie Alchemie erscheint, ist die bildliche Anwendung der mathematischen Identität

$$(10 + x)(10 + y) = 10(10 + x + y) + xy, \tag{40}$$

oder allgemeiner, wobei s einen „schönen“ Multiplikator bezeichne,

$$(s + x)(s + y) = s(s + x + y) + xy. \tag{41}$$

“Dead Reckoning”

Diese bildliche Berechnung wurde früher Schulkindern beigebracht, wenn die Multiplikation zweier Zahlen größer als 5 erfolgen sollte. Hier noch als Beispiele $8 \cdot 9$ und $9 \cdot 9$:

$$\begin{array}{ccccc} 8 & & 9 & & \\ & \searrow & - & & \\ 1 & \cdot & 2 & = & \boxed{2} \\ \hline & = & \boxed{7} & & \end{array} \qquad \begin{array}{ccccc} 9 & & 9 & & \\ & \searrow & - & & \\ 1 & \cdot & 1 & = & \boxed{1} \\ \hline & = & \boxed{8} & & \end{array} \tag{42}$$

Als Warnung: Manchmal muss man noch Nachbearbeiten. Dazu sehen wir uns $6 \cdot 7$ an:

$$\begin{array}{ccccc} 6 & & 7 & & \\ & \searrow & - & & \\ 3 & \cdot & 4 & = & \boxed{12} \\ \hline & = & \boxed{3} & & \end{array} \tag{43}$$

Das Endergebnis ist $10 \cdot 3 + 12 = 42$. Was auch sonst.

“Dead Reckoning”

Schnelles und gutes Kopfrechnen basiert auf solchen Beobachtungen und viel Übungen, so sollte man keine Probleme haben, zwei zweistellige Zahlen im Kopf auf einmal zu multiplizieren.

Die Primfaktoren der Basis, in der wir rechnen, sind auch sehr interessant: Hier gilt ja $10 = 2 \cdot 5$. Damit sind Multiplikationen mit oder Divisionen durch 5 zurückführbar auf Divisionen durch oder Multiplikationen mit 2:

$$234 \cdot 5 = 234 \cdot 10/2 = 2340/2 = (2.34.0)/2 = (1.17.0) = 1170, \qquad (44)$$

oder

$$235/5 = 235 \cdot 2/10 = (2|3|5) \cdot 2/10 = (4|6|10)/10 = (4|7|0)/10 = 47, \qquad (45)$$

wobei die Punkte zwischen den Ziffernblöcken eine Einteilung in Ziffernblöcke zu geraden Zahlen und die senkrechten Striche eine Aufteilung in einzelne Ziffern mit möglichem Überlappen bedeuten.

“Dead Reckoning”

Aber auch Zahlen nahe einer Zehnerpotenz sind hilfreich: So kann man (implizite) Multiplikationen mit $9 = 10 - 1$ ausnutzen. Als Beispiel dazu:

$$\begin{aligned} 36 \cdot 157 = 9 \cdot 4 \cdot 157 &= (10-1) \cdot 4 \cdot (150+7) \\ &= (10-1) \cdot (400 + 400/2 + 2 \cdot 2 \cdot 7) \\ &= (10-1) \cdot 628 = 6280 - 628 \\ &= (6|2 - 6|8 - 2|0 - 8) = (6| - 4|6| - 8) \\ &= (6| - 4|5|2) = (5|6|5|2) = 5652. \end{aligned} \tag{46}$$

In Zweiergruppen gerechnet geht das Ganze dann so:

$$6280 - 628 = (62|_2 80) - (6|_2 28) = (56|_2 52) = 5652. \tag{47}$$

In Dreiergruppen:

$$6280 - 628 = (6|_3 280) - (628) = (6|_3 - 348) = (5|652) = 5652. \tag{48}$$

“Dead Reckoning”

Multiplikationen mit 11 oder 111 oder ähnlich sind auch sehr strukturiert und sehr schnell berechenbar. In den nichtnormalisierten Ziffern des Ergebnisses tauchen die Ziffern des Multiplikanden genausooft auf, wie Einsen in der Zahl sind. Die resultierende Vereinfachung kann man auch für deren Primfaktoren nutzen: So gilt $111 = 37 \cdot 3$, was man sich vielleicht merken sollte, aber auch $1111 = 11 \cdot 101$ und $111111 = 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 = 111 \cdot 7 \cdot 11 \cdot 13 = 111 \cdot 11 \cdot 91$.

Damit kann man zum Beispiel wie folgt rechnen:

$$\begin{aligned} 37 \cdot 253 = 111 \cdot 253/3 &= (2|2+5|2+5+3|5+3|3)/3 \\ &= (2|7|10|8|3)/3 = (27:108:3)/3 \\ &= (9:36:1) = 9361. \end{aligned} \tag{49}$$

Hier bedeutet die Doppelpunktnotation, dass die Ziffernblöcke zu durch 3 teilbaren Zahlen zusammengruppiert wurden. Hier ist wieder Vorsicht bei Überlappungen geboten.

“Dead Reckoning”

Es bietet sich an, viele Quadratzahlen auswendig zu können, da

$$38 \cdot 32 = (35)^2 - (3)^2, \qquad 62 \cdot 74 = (68)^2 - (6)^2, \tag{50}$$

oder eben allgemein

$$a \cdot b = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 \tag{51}$$

gilt. Wenn das arithmetische Mittel also eine ganze Zahl ist, kann man diesen Trick, genannt “Rule of Quarter Squares”, leicht anwenden. Ansonsten rechnet man wirklich die Quadrate von $a+b$ und $a-b$ aus und teilt die Differenz durch 4.

Quadratzahlen lassen sich schnell auswendig lernen, wenn man an die Bildung als Summe der ersten ungeraden Zahlen denkt: Es gilt

$$\begin{aligned} (n+1)^2 - n^2 &= n + (n+1), \quad \text{also z. B.} \\ 13^2 = 12^2 + (12+13) &= 144 + 25 = 169. \end{aligned} \tag{52}$$

“Dead Reckoning”

Quadratzahlen, welche auf 5 enden, lassen sich leicht berechnen:

$$(a|5)^2 = a \cdot (a+1)|_2 25, \qquad (35)^2 = 3 \cdot 4|_2 25 = 1225. \tag{53}$$

Das folgt sofort aus

$$\begin{aligned}(a|5)^2 = (a \cdot 10 + 5)^2 &= a^2 \cdot 100 + 2a \cdot 10 \cdot 5 + 5^2 \\ &= a(a+1) \cdot 100 + 25.\end{aligned} \tag{54}$$

Demnach ist 555^2 schnell berechnet:

$$\begin{aligned}555^2 = (55 \cdot (55+1))|_2 25 &= (55^2 + 55)|_2 25 \\ &= (5 \cdot 6|_2 25 + 55)|_2 25 \\ &= 30|_2 (25 + 55)|_2 25 = 308025.\end{aligned} \tag{55}$$

“Dead Reckoning”

Bei anderen Aufgaben, wie zum Beispiel

$$62 \cdot 74 = (68)^2 - (6)^2 \tag{56}$$

nutzt man eine Umschreibung „in die andere Richtung“:

$$\begin{aligned} 68^2 &= 70 \cdot 66 + 4 = (7 \cdot 6) \cdot 11 \cdot 10 + 4 \\ &= (42 \cdot 11)|0 + 4 = (4|(4+2)|2)|4 = 4624. \end{aligned} \tag{57}$$

Die dahinterstehende Regel mit einem „schönen“ Multiplikator s ist

$$68^2 = (s+d)^2 = s \cdot (s+2d) + d^2 = (70-2)^2 = 70 \cdot (68-2) + (-2)^2. \tag{58}$$

Das Vorzeichen in der Regel der geviertelten Quadrate merkt man sich leicht aufgrund der Ungleichung zwischen dem geometrischen und dem arithmetischen Mittel. Um das Quadrat des geometrischen Mittels zu erhalten, also das Produkt der beiden Zahlen, muss man das Quadrat des arithmetischen Mittels verkleinern, also eine Quadratzahl abziehen.

“Dead Reckoning”

Wenn schon bekannt ist, das eine Zahl die Potenz einer ganzen Zahl ist, so läßt sich diese schnell berechnen. Als Beispiel betrachten wir die Aufgabe, n mit

$$n^5 = 66577793506607 \tag{59}$$

zu berechnen, wobei die Metainformation, dass $n \in \mathbb{N}$, eingeht.

Die Lösung ist in der Größenordnung von 300, da (wir aus Tabellen wissen dass) $300^5 = 243 \cdot 10^{10}$ und $400^5 = 1024 \cdot 10^{10}$. Also suchen wir nach zwei Ziffern: $n = (3|a|b)$.

Die letzte gesuchte Ziffer der Basis ist bei Exponenten der Form $4k + 1$ immer gleich der letzten Ziffer des gegebenen Wertes der Potenz. Also wissen wir schon, dass $n = (3|a|7)$.

Mit ein wenig Wissen und sehr wenig Berechnungen haben wir bereits zwei von drei Ziffern!

“Dead Reckoning”

Jetzt verwenden wir die Teilung durch 9 mit Rest: Der Rest von n nach Teilung durch 9 steht mit dem Rest der Teilung von n^5 durch 9 in Verbindung, man überlegt sich schnell, dass

$n \mod 9$	0	1	2	3	4	5	6	7	8
$n^5 \mod 9$	0	1	5	0	7	2	0	4	8

(60)

gilt. Zum Beispiel gilt

$$\begin{aligned} 5^2 \bmod 9 &= 25 \bmod 9 = (18+7) \bmod 9 = 7, \\ 5^4 \bmod 9 &= 7^2 \bmod 9 = (45+4) \bmod 9 = 4, \\ 5^5 \bmod 9 &= (5 \cdot 4) \bmod 9 = (18+2) \bmod 9 = 2. \end{aligned} \tag{61}$$

Genau so eine Tabelle kann man auch für die Teilung mit Rest durch 11 aufstellen. Diese wird dann manchmal zusätzlich verwendet, insbesondere wenn $n^5 \bmod 9 = 0$ ist, welches nicht eindeutig die Teilbarkeit durch 9 von n erklärt.

“Dead Reckoning”

Nun gilt

$$\begin{aligned}
&6657793506607 \bmod 9 \\
&\quad = (6+6+5+7+7+9+3+5+0+6+6+0+7) \bmod 9 \\
&\quad = (6+5+7+7+5+6+6+7) \bmod 9 \qquad (62)\\
&\quad = (5+7+7+5+7) \bmod 9 \\
&\quad = (3\cdot 7 + 2\cdot 5) \bmod 9 = 31 \bmod 9 = (27+4) \bmod 9 = 4,
\end{aligned}$$

also muss nach der eben erstellten Tabelle

$$n \bmod 9 = (3|a|7) \bmod 9 = 7 \qquad (63)$$

gelten, also

$$0 = (n-7) \bmod 9 = ((3+a+7)-7) \bmod 9 = (3+a) \bmod 9, \qquad (64)$$

also $3+a$ ohne Rest durch 9 teilbar sein. Damit bleibt nur $a = 6$ und $n = 367$.

Vorwissen

Definition (natürliche Zahlen)

Die Menge $\mathbb{N} = \{1, 2, 3, ...\}$ der natürlichen Zahlen ist definiert durch die folgenden 5 Peano-Axiome:

$$1 \in \mathbb{N} \tag{65}$$

$$\forall\, n \in \mathbb{N}\ \exists!\, n' \in \mathbb{N} \tag{66}$$

$$\forall\, n \in \mathbb{N} : 1 \neq n' \tag{67}$$

$$\forall\, n, m \in \mathbb{N} : n' = m' \Rightarrow n = m \tag{68}$$

$$\forall\, M \subset \mathbb{N} : (1 \in M \wedge \forall\, n \in M \Rightarrow n' \in M) \Rightarrow M = \mathbb{N} \tag{69}$$

Bemerkung

Das Axiom (69) *ist das sogenannte Induktionsaxiom.*

Vorwissen

Definition (Addition natürlicher Zahlen)

Die Addition $(+)$ natürlicher Zahlen $m, n \in \mathbb{N}$ ist definiert durch

$$n + 1 := n', \qquad n + m' := (n + m)'. \tag{70}$$

Definition (Multiplikation natürlicher Zahlen)

Die Multiplikation $(\cdot)$ natürlicher Zahlen $m, n \in \mathbb{N}$ ist definiert durch

$$n \cdot 1 := n, \qquad n \cdot m' := (n \cdot m) + n. \tag{71}$$

Übungsaufgabe

Man beweise, dass die so definierten Operationen Addition und Multiplikation kommutativ, assoziativ und distributiv sind und mit den bereits “bekannten” Operationen übereinstimmen.

Vorwissen

Definition (Teilbarkeit)

Eine Zahl $n \in \mathbb{N}$ heißt teilbar durch $m \in \mathbb{N}$, in Zeichen $m|n$, wenn es ein $x \in \mathbb{N}$ gibt mit $mx = n$.

Definition (Primzahl)

Eine Primzahl $p \in \mathbb{N}$ ist eine Zahl, deren Menge der Teiler die Mächtigkeit zwei hat, in Zeichen

$$\mathbb{P} := \{p \in \mathbb{N} : \#\{x : x|p\} = 2\}, \tag{72}$$

wobei $\mathbb{P}$ im Folgenden die Menge der Primzahlen bezeichne.

Bemerkung

Damit ist Eins keine Primzahl.

Vorwissen

Definition (Primteiler)

Ein Primteiler p einer Zahl n ist ein Teiler von n, der eine Primzahl ist.

Theorem

Jede natürliche Zahl ungleich Eins hat Primteiler.

Beweis.

Übungsaufgabe. □

Theorem

Eins hat keine Primteiler.

Beweis.

Die Mächtigkeit der Menge der Teiler ist gleich Eins. □

Euklid: Beweis durch Widerspruch

Theorem

Es gibt unendlich viele Primzahlen.

Beweis durch Widerspruch.

Angenommen, es gäbe endlich viele Primzahlen $p_1, \ldots, p_n$. Dann hat die Zahl

$$c = \prod_{i=1}^{n} p_i + 1 \tag{73}$$

keine der Zahlen p_i als Teiler. Sei p ein Primteiler von c. Dann unterscheidet sich p von allen bisher bekannten p_i, da sonst $p|c$ und $p|\prod p_i$ und damit $p|1$, was laut Annahme nicht sein kann. □

Vorwissen

Theorem (Eindeutigkeit und Existenz der Primfaktorzerlegung)

Für alle $n \in \mathbb{N}$ existiert eine eindeutige Primfaktorzerlegung

$$n = \prod_{i=1}^{\ell} p_i^{k_i}, \quad p_1 < p_2 < \cdots < p_\ell \leqslant n, \tag{74}$$

wobei $p_i \in \mathbb{P}$ paarweise verschiedene endlich viele ($\ell \in \mathbb{N}_0$ Stück) Primzahlen sind, und $k_i \in \mathbb{N}$ deren Vielfachheit angibt. ($\prod_{i=1}^{0} a_i := 1$)

Beweis.

Da jede Zahl Primteiler hat, und Primzahlen grösser gleich 2 sind, folgt, dass die rekursive Konstruktion der Primfaktorzerlegung durch sukzessives Teilen durch einen Primteiler terminiert. Das beweist die Existenz.

Die Eindeutigkeit folgt aus der Teilbarkeitsrelation, denn seien zwei Primfaktorzerlegungen $n = \prod_{i=1}^{\ell} p_i^{k_i} = \prod_{j=1}^{m} q_j^{k_j}$ gegeben, dann sind auch alle enthaltenen Primzahlpotenzen Teiler beider Zerlegungen. □

Vorwissen

Definition (natürlicher Logarithmus)

Der natürliche Logarithmus $\ln$ sei definiert über die Integration

$$\ln(x) := \int_1^x \frac{dt}{t}. \tag{75}$$

Bemerkung

Aus der Definition ist ersichtlich, dass $\ln(x)$ *unbeschränkt wächst, in Zeichen* $\lim_{x\to\infty} \ln(x) = \infty$.

Definition (Primzahlzählfunktion)

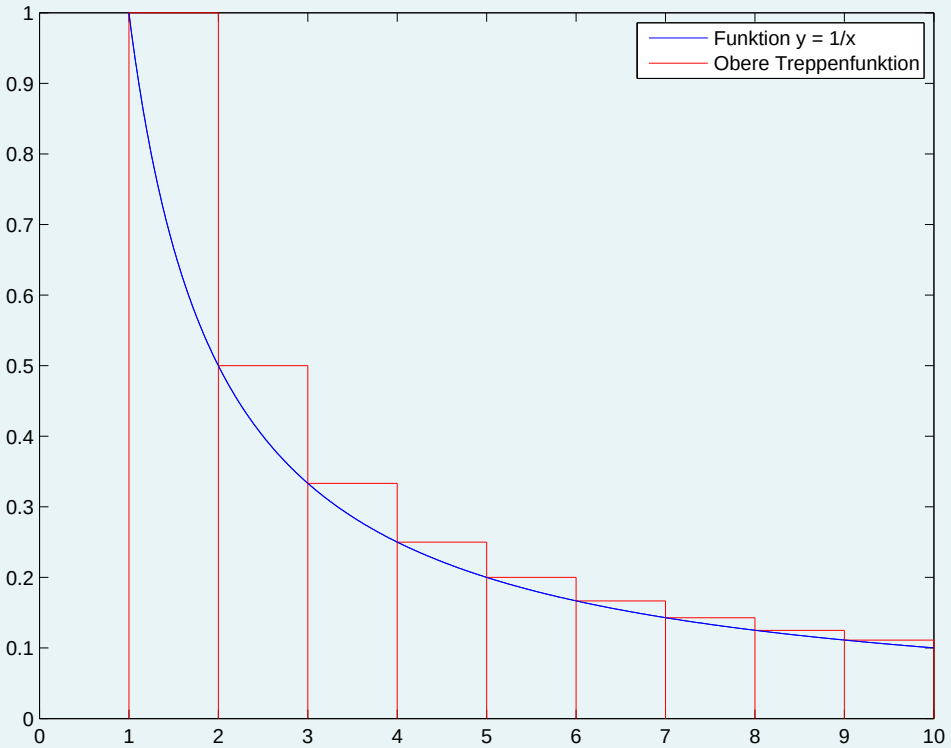
Wir definieren für alle $x \in \mathbb{R}$ die Primzahlzählfunktion π durch

$$\pi(x) := \#\{p \leqslant x \,:\, p \in \mathbb{P}\}. \tag{76}$$

Vorwissen

Bemerkung (zur Integration)

Obere Treppenfunktionen geben leicht berechenbare obere Schranken:



Vorwissen

Lemma

Die geometrische Reihe

$$G(q) := \sum_{k=0}^{\infty} q^k \tag{77}$$

konvergiert, wenn $|q| < 1$. *Der Grenzwert ist durch* $(1-q)^{-1}$ *gegeben.*

Beweis.

Die Reihe ist der Limes der endlichen Summe

$$G_n(q) := \sum_{k=0}^{n} q^k = 1 + q + q^2 + q^3 + \cdots + q^n. \tag{78}$$

Nun gilt $(1-q)G_n(q) = G_n(q) - qG_n(q) = 1 - q^{n+1}$, und da $|q| < 1$ folgt mit $\lim_{n\to\infty} q^{n+1} = 0$ das Lemma. □

Euler: Beweis mit Mitteln der Analysis

Theorem

Für alle $x \in \mathbb{R}_+$ *gilt* $\ln(x) \leqslant \pi(x) + 1$.

Beweis.

Aus der Definition des Logarithmus folgt mit einer oberen Treppenfunktion

$$\ln(x) \leqslant 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} \leqslant \sum{}' \frac{1}{m}, \quad n \leqslant x < n+1, \tag{79}$$

wobei die Summierung über alle $m \in \mathbb{N}$ *erfolgt, so dass nur Primfaktoren* $p \leqslant x$ *enthalten sind. Jedes solche* m *kann auf eindeutige Weise geschrieben werden als* $m = \prod_{p \leqslant x} p^{k_p}$*, damit gilt dann*

$$\ln(x) \leqslant \sum{}' \frac{1}{m} = \prod_{p \in \mathbb{P}, p \leqslant x} \left(\sum_{k \geqslant 0} \frac{1}{p^k} \right). \tag{80}$$

Euler: Beweis mit Mitteln der Analysis

Beweis.

Die innere Summe ist eine geometrische Reihe mit Faktor $1/p < 1$, woraus

$$\ln(x) \leqslant \prod{}' \frac{1}{1-\frac{1}{p}} = \prod{}' \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1} \tag{81}$$

folgt. Da trivialerweise $p_k \geqslant k+1$ gilt (wenn Primzahlen aufeinander folgen würden, wäre $p_k = k+1$, da Eins keine Primzahl ist), folgt weiter

$$\frac{p_k}{p_k - 1} = 1 + \frac{1}{p_k - 1} \leqslant 1 + \frac{1}{k} = \frac{k+1}{k}. \tag{82}$$

Daraus folgt

$$\ln(x) \leqslant \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x) + 1. \tag{83}$$

□

Euler: Beweis mit Mitteln der Analysis

Theorem

Es gibt unendlich viele Primzahlen.

Beweis.

Da der Logarithmus nicht beschränkt ist, folgt, dass auch $\pi(x)$ über alle Grenzen wächst, damit existieren unendlich viele Primzahlen. □

Der Fundamentalsatz der Algebra

Der in diesem Abschnitt behandelte Fundamentalsatz der Algebra wird in der folgenden Form behandelt:

Theorem (Fundamentalsatz der Algebra)

Jedes nichtkonstante Polynom p mit Koeffizienten in $\mathbb{C}$ hat eine Nullstelle $z \in \mathbb{C}$.

Manchmal ist es leichter, nur Polynome mit Koeffizienten aus den reellen Zahlen zu betrachten. Dieses stellt keine wesentliche Einschränkung dar:

Lemma

Ist c eine Nullstelle des reellen Polynomes $P(z) = \overline{p(\overline{z})}p(z)$, dann ist c oder $\overline{c}$ eine Nullstelle des komplexen Polynomes $p(z)$.

Vorwissen

Es folgen einige Resultate ohne Beweis.

Lemma (Dreiecksungleichung; Definitheit)

Der Absolutbetrag in $\mathbb{C}$ hat folgende Eigenschaften:

Dreiecksungleichung: *Für $z, w \in \mathbb{C}$ gilt $||z| - |w|| \leqslant |z \pm w| \leqslant |z| + |w|$.*

Definitheit: *Aus $|z| = 0$ folgt $z = 0$.*

Definition (Polynom)

Ein Polynom vom Grad n mit Koeffizienten $a_i \in \mathbb{K}$, $i = 0, 1, \ldots, n$ in einem Körper $\mathbb{K}$ ist eine Funktion p der Gestalt

$$p(z) = \sum_{k=0}^{n} a_k z^k = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0, \quad a_n \neq 0. \tag{84}$$

Vorwissen

Definition (Stetigkeit)

Eine Funktion $f : D \to \mathbb{C}$ heißt stetig in z, wenn

$$\forall\, \epsilon > 0\ \exists\, \delta > 0\ :\ |f(w) - f(z)| < \epsilon\ \forall\ |w - z| < \delta. \tag{85}$$

Eine Funktion heißt stetig, wenn sie in jedem Punkt des Definitionsbereiches stetig ist.

Theorem (Satz vom Minimum und Maximum: Weierstraß)

Jede stetige Funktion $f : K \to \mathbb{R}$ auf einem Kompaktum K nimmt ein Maximum und ein Minimum an, d.h., es gibt ein $\xi_1 \in K$ und ein $\xi_2 \in K$, so dass für alle $x \in K$

$$f(\xi_1) \leqslant f(x) \leqslant f(\xi_2) \tag{86}$$

gilt.

Vorwissen

Lemma (Polarkoordinaten)

Jede komplexe Zahl $c \neq 0$ läßt sich in eindeutiger Weise in sogenannten Polarkoordinaten (r, φ) darstellen gemäß

$$c = r(\cos(\varphi) + i\sin(\varphi)) = re^{i\varphi}, \quad \textit{wobei} \quad r = |c| \in \mathbb{R}_+, \varphi \in (-\pi, \pi]. \tag{87}$$

Beweis.

Dieses sieht man wie folgt. Es ist laut Lemma nur noch φ zu bestimmen. Sei

$$\frac{c}{|c|} = \xi + i\eta, \quad \xi, \eta \in \mathbb{R}. \tag{88}$$

Dann gilt $|\xi + i\eta|^2 = \xi^2 + \eta^2 = 1$. Setze nun $\alpha = \arccos(\xi)$. Dann gilt $\xi = \cos(\alpha)$ und zumindest $\eta = \pm\sin(\alpha)$. Wir setzen $\varphi = \alpha$, wenn $\eta = \sin(\alpha)$ und $\varphi = -\alpha$ sonst. Es gilt $\cos(-\alpha) = \cos(\alpha)$ und $\sin(-\alpha) = -\sin(\alpha)$. □

Vorwissen

Lemma (Existenz von k-ten Wurzeln)

Die Gleichung $z^k = c$ mit beliebigem festen $c \in \mathbb{C}$ hat eine Lösung.

Beweis.

Jede komplexe Zahl $c \neq 0$ läßt sich in Polarkoordinaten als $c = |c|e^{i\varphi}$ darstellen. Die Zahl

$$\sqrt[k]{c} := \sqrt[k]{|c|}e^{i\varphi/k} \tag{89}$$

leistet das Gewünschte. Wenn $c = 0$ ist 0 eine Lösung. □

Argand: Beweis durch Minimierung

Im Folgenden sei $p(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$ mit $n > 1$.

Lemma (Existenz des Minimums)

Die Funktion $|p|$ nimmt auf $\mathbb{C}$ ein Minimum an.

Beweis.

Sei r definiert als $r := 1 + |a_{n-1}| + \cdots + |a_0|$. Dann gilt für $|z| \geqslant r \geqslant 1$

$$
\begin{aligned}
|p(z)| &\geqslant |z|^n - \left(|a_{n-1}||z|^{n-1} + \cdots + |a_1||z| + |a_0|\right) && (90)\\
&\geqslant |z|^n - \left(|a_{n-1}| + \cdots + |a_1| + |a_0|\right)|z|^{n-1} && (91)\\
&\geqslant |z|^n - (r-1)|z|^{n-1} \geqslant |z|^n - (|z|-1)|z|^{n-1} = |z|^{n-1} \geqslant r^{n-1} \geqslant r. && (92)
\end{aligned}
$$

Die Funktion $|p|$ nimmt auf der berandeten Kreisscheibe $\overline{K_r(0)}$ nach dem Satz von Weierstraß ein Minimum an. Da $|p(0)| = |a_0| < r$, ist dieses Minimum das globale Minimum auf ganz $\mathbb{C}$. □

Argand: Beweis durch Minimierung

Lemma (Negative Charakterisierung des Minimums)

Sei $|p(z_0)| \neq 0$. Dann ist z_0 kein Minimum, d.h., es gibt ein z_1 mit

$$|p(z_1)| < |p(z_0)|. \tag{93}$$

Beweis.

Sei

$$s(w) := \frac{p(z_0 + w)}{p(z_0)} = 1 + bw^k + \cdots . \tag{94}$$

Sei β eine k-te Wurzel von $-b^{-1}$. Dann gilt

$$q(x) := s(\beta x) =: 1 - x^k + Q(x) =: 1 - x^k + x^{k+1}R(x). \tag{95}$$

Sei $C > 0$ eine obere Schranke für $|R|$ auf $\overline{K_1(0)}$. Dann gilt

$$|Q(x)| \leqslant C|x|^{k+1}, \quad |x| \leqslant 1, \tag{96}$$

Argand: Beweis durch Minimierung

Beweis.

und daher

$$|Q(x)| \leqslant |x|^k, \quad 0 < |x| < \min(1, C^{-1}). \tag{97}$$

Für reelle x_0 mit $0 < x_0 < \min(1, C^{-1})$ folgt nun

$$|q(x_0)| \leqslant 1 - x_0^k + |Q(x_0)| < 1 - x_0^k + x_0^k = 1. \tag{98}$$

Das bedeutet wiederum $|s(\beta x_0)| < 1$ und damit

$$|p(z_0 + \beta x_0)| < |p(z_0)|. \tag{99}$$

Setzen von $z_1 = z_0 + \beta x_0$ vollendet den Beweis. □

Argand: Beweis durch Minimierung

Theorem (Fundamentalsatz der Algebra)

Jedes nichtkonstante Polynom p mit Koeffizienten in $\mathbb{C}$ hat eine Nullstelle $z \in \mathbb{C}$.

Beweis.

Nach dem ersten Lemma nimmt $|p(z)|$ ein Minimum an, nach dem zweiten Lemma geben Punkte $z_0 \in \mathbb{C}$ mit $|p(z_0)| \neq 0$ kein Minimum. Damit ist das Minimum gleich 0. Nach dem ersten Lemma existiert daher ein Punkt $z_1 \in \mathbb{C}$ mit $|p(z_1)| = 0$, also aufgrund der Definitheit des Absolutbetrages auch mit $p(z_1) = 0$. □

Der Satz von Feit und Thompson

Der Satz von Feit und Thompson (Feit and Thompson, 1963) ist recht kurz. Er besagt:

Alle endlichen Gruppen ungerader Ordnung sind auflösbar.

Um ihn zu verstehen, muss man nur wenige Begriffe der Algebra verstehen, vor allem, was eine Gruppe ist, und was Auflösbarkeit bedeutet. Wir halten uns dabei ungefähr an (Meyberg, 1975).

Eine Gruppe ist eine Menge G mit einer Verknüpfung

$$\circ : \begin{cases} G \times G & \to & G, \\ (x, y) & \mapsto & x \circ y, \end{cases} \tag{100}$$

die den folgenden Regeln (Axiomen) genügt:

$$\forall\, a, b, c \in G : (a \circ b) \circ c = a \circ (b \circ c), \qquad \text{(Assoziativität)}$$

$$\exists\, e \in G\, \forall\, g \in G : e \circ g = g, \qquad \text{(Neutrales Element)}$$

$$\forall\, g \in G\, \exists\, h \in G : h \circ g = e. \qquad \text{(Inverses Element)}$$

Der Satz von Feit und Thompson

Wenn zusätzlich noch

$$\forall\, a, b \in G : a \circ b = b \circ a \qquad \text{(Kommutativität)}$$

gilt, so nennt man die Gruppe $(G, \circ)$ eine kommutative oder abelsche Gruppe.

Eine Gruppe wird oft statt mit $\circ$ oft mit dem Multiplikationspunkt $\cdot$ geschrieben, das neutrale Element dann als Eins bezeichnet und als 1 geschrieben, das Inverse zu $g \in G$ wird dann mit $g^{-1} \in G$ bezeichnet.

Eine abelsche Gruppe schreibt man oft mit dem Zeichen $+$ statt $\circ$, dann wird das neutrale Element als Null bezeichnet und mit dem Symbol 0 gekennzeichnet, das Inverse zu $g \in G$ wird dann mit $-g$ bezeichnet.

$(U, \circ)$ mit einer Untermenge $U \subset G$ heißt Untergruppe, wenn mit $a, b \in U$ auch wieder $a \circ b^{-1} \in U$, wobei b^{-1} das inverse Element zu $b \in U$ bezeichnet.

Der Satz von Feit und Thompson

Die Anzahl verschiedener Elemente in einer Gruppe ist die Gruppenordnung. Besteht eine Gruppe nur aus endlich vielen Elementen, so nennt man die Gruppe endlich.

Damit haben wir nahezu alle Einzelheiten aus dem Satz von Feit und Thompson übersetzt:

Alle endlichen Gruppen ungerader Ordnung sind auflösbar.

Es fehlt der Begriff der Auflösbarkeit. Dazu benötigen wir die Begriffe der erzeugten Gruppe, des Kommutators und der Kommutatorgruppe.

Historisch gesehen wurde die Gruppentheorie ins Leben gerufen, als die Leute nach Auflöseformeln für Polynome vom Grad größer gleich fünf suchten, analog zu den Formeln von Cardano. Diese sind eng verknüpft mit dem Begriff der Auflösbarkeit.

Der Satz von Feit und Thompson

Definition (erzeugte Gruppe)

Es sei $S \subset G$. Dann ist der Durchschnitt aller Untergruppen U mit $S \subset U \subset G$ eine Untergruppe

$$\langle S \rangle := \bigcap \{U \mid U \text{ ist Untergruppe von } G \text{ mit } S \subset G\}, \tag{101}$$

die von S erzeugte Gruppe.

Die von S erzeugte Gruppe $\langle S \rangle$ ist quasi die kleinste Untergruppe von G, welche S enthält. Falls S schon Untergruppe ist, ist natürlich $\langle S \rangle = S$. Falls nicht, dann können ja nur Elemente fehlen, die mittels der Gruppenaxiome aus Elementen von S hervorgegangen sind:

Theorem (Charakterisierung der erzeugten Gruppe)

Ist G eine Gruppe und S eine nichtleere Teilmenge von G, dann besteht $\langle S \rangle$, die von S erzeugte Untergruppe, aus allen endlichen Produkten von Elementen aus $S \cup S^{-1}$.

Der Satz von Feit und Thompson

Definition (Kommutator; Kommutatorgruppe)

Der Kommutator zweier Elemente $a, b \in G$ ist definiert als

$$[a, b] := aba^{-1}b^{-1}. \tag{102}$$

Die von allen Kommutatoren erzeugte Gruppe

$$K(G) := \langle \{[a, b] \mid a, b \in G\} \rangle \tag{103}$$

wird Kommutatorgruppe genannt. Dieser Prozess kann iteriert werden, wir definieren die höheren Kommutatorgruppen induktiv durch $K_0(G) := G$, $K_{n+1}(G) := K(K_n(G))$, $n \geqslant 0$.

Definition (Auflösbarkeit)

Eine Gruppe heißt auflösbar, wenn es ein $n \in \mathbb{N}$ gibt mit $K_n(G) = \{e\}$.

Der Satz von Feit und Thompson

Jede abelsche Gruppe ist auflösbar, da alle Kommutatoren aus dem neutralen Element bestehen,

$$[a,b] = aba^{-1}b^{-1} = baa^{-1}b^{-1} = beb^{-1} = bb^{-1} = e, \tag{104}$$

und somit $K_1(G) = K(G) = \{e\}$ gilt. In diesem Sinne sind auflösbare Gruppen Verallgemeinerungen von abelschen Gruppen.

Soweit zum Verständnis der Aussage des Satzes.

Um den Satz zu beweisen, haben Feit und Thompson zuerst einmal viele andere Definitionen auflisten müssen, zuerst etwa 55 Definitionen, gefolgt von unzähligen anderen Definitionen und dann vielen Hilfssätzen.

Ihr Beweis benötigt 255 Seiten, eine ganze Ausgabe zu vier Bänden eines mathematischen Journals.

Der große Satz

Der Beweis wurde später zwar an einigen Stellen vereinfacht, bildet aber selbst nur eine kleine der vielen Grundlagen des sogenannten großen Satzes (der Gruppentheorie).

Der große Satz beschreibt die

> *Klassifikation der endlichen einfachen Gruppen.*

Der Gesamt„beweis“ wird nicht von allen Mathematikern anerkannt, wir geben ohne Übersetzung die Einleitung aus (Gorenstein et al., 1994) wieder, um zu erklären, wieso:

> *The existing proof of the classification of the finite simple groups runs to somewhere between 10,000 and 15,000 journal pages, spread across some 500 separate articles by more than 100 mathematicians, almost all written between 1950 and the early 1980's.*

Wir geben im Folgenden daher nur den Beweis für den Satz von Feit und Thompson wieder.

Der Beweis

Zuerst folgt die verwendete Notation:

- $\langle \cdots \mid \cdots \rangle$: Die Gruppe erzeugt von $\cdots$ so dass $\cdots$
- $\{ \cdots \mid \cdots \}$: Die Menge von $\cdots$ so dass $\cdots$
- $gp\langle \cdots \mid \cdots \rangle$: Die Gruppe erzeugt durch die Generatoren $\cdots$ so dass $\cdots$
- $|\mathfrak{X}|$: Die Anzahl der Elemente in $\mathfrak{X}$
- $\mathfrak{X}^{\#}$: Die Menge der Nicht-Identitäts-Elemente in $\mathfrak{X}$
- π: Eine Menge von Primzahlen. Wenn $\pi = \{p\}$, identifizieren wir π mit p
- π': Die komplementäre Menge von Primzahlen
- π-Zahl: Eine Zahl ungleich Null, deren Primfaktoren alle in π liegen
- n_π: Die größte π-Zahl, die die Zahl $n \in \mathbb{N}$ teilt

Ok, das ist jetzt nicht mehr ernst gemeint. Viel Spaß beim weiteren Studium!

Wir sehen uns am Freitag, den 29. bei der Anleitung zur Mathematik I :-)

Aigner, M. and Ziegler, G. M. (1999).
Proofs from The Book.
Springer-Verlag, Berlin.
Including illustrations by Karl H. Hofmann, Corrected reprint of the 1998 original.

Doerfler, R. W. (1993).
Dead Reckoning: Calculating Without Instruments.
Gulf Publishing.

Feit, W. and Thompson, J. G. (1963).
Solvability of groups of odd order.
Pacific J. Math., 13:775–1029.

Gorenstein, D., Lyons, R., and Solomon, R. (1994).
The classification of the finite simple groups, volume 40 of *Mathematical Surveys and Monographs*.
American Mathematical Society, Providence, RI.

Königsberger, K. (2004).
Analysis. 1.
Springer-Lehrbuch. [Springer Textbook]. Springer-Verlag, Berlin, sixth edition.

Mahajan, S. (2010).
Street-fighting mathematics.
MIT Press, Cambridge, MA.
With a foreword by Carver A. Mead, The art of educated guessing and opportunistic problem solving.

Meyberg, K. (1975).
Algebra. Teil 1.
Carl Hanser Verlag, Munich.
Mathematische Grundlagen für Mathematiker, Physiker und Ingenieure.

Polya, G. (2004).

How to solve it.

Princeton Science Library. Princeton University Press, Princeton, NJ. A new aspect of mathematical method, Expanded version of the 1988 edition, with a new foreword by John H. Conway.

Sticker, H. (2000).

How to Calculate Quickly: Full Course in Speed Arithmetic.

Dover.