GERMAN EXAM – FALL QUARTER 2005

Axiomatischer Aufbau

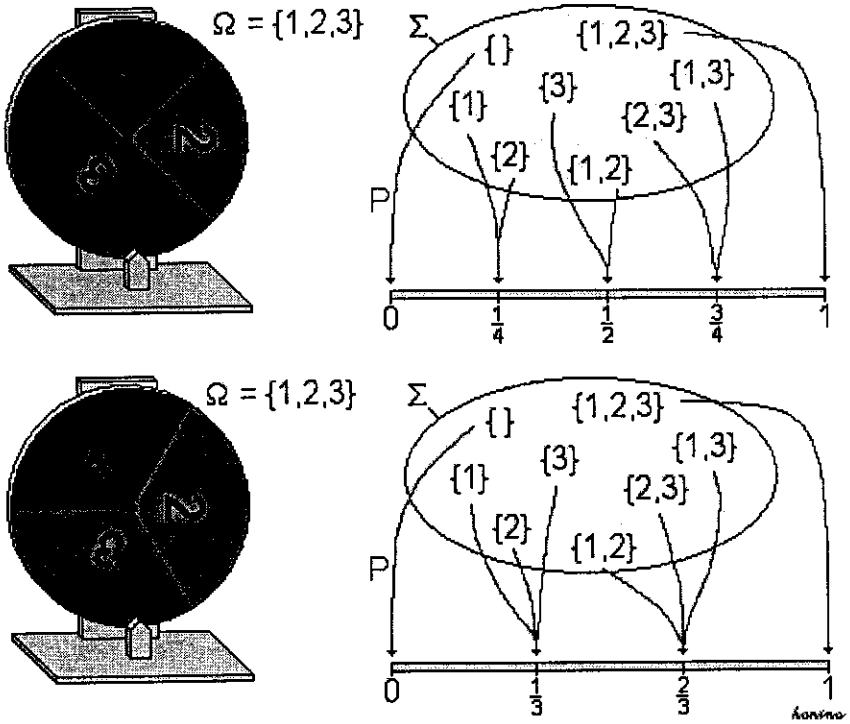
Wie jedes Teilgebiet der modernen Mathematik wird auch die Wahrscheinlichkeitstheorie mengentheoretisch formuliert und auf axiomatische Vorgaben aufgebaut. Ausgangspunkt der Wahrscheinlichkeitstheorie sind *Ereignisse,* die als Mengen aufgefasst werden und denen Wahrscheinlichkeiten zugeordnet sind; Wahrscheinlichkeiten sind reelle Zahlen zwischen 0 und 1; die Zuordnung von Wahrscheinlichkeiten zu Ereignissen muss gewissen Mindestanforderungen genügen.

Diese Definitionen geben keinen Hinweis, wie man die Wahrscheinlichkeiten einzelner Ereignisse ermitteln kann; sie sagen auch nichts darüber aus, was Zufall und was Wahrscheinlichkeit eigentlich sind. Die mathematische Formulierung der Wahrscheinlichkeitstheorie ist somit für verschiedene Interpretationen offen. Siehe dazu die Artikel Wahrscheinlichkeit, Bayesscher Wahrscheinlichkeitsbegriff, Frequentistischer Wahrscheinlichkeitsbegriff, Quantenlogik.

Definitionen

Konzeptionell wird von einem Zufallsvorgang oder Zufallsexperiment ausgegangen. Alle möglichen Ergebnisse dieses Zufallsvorgangs fasst man in der Ergebnismenge Ω zusammen. Wenn ein bestimmtes Ergebnis eintritt, spricht man von einem *Ereignis*. Das Ereignis ist als Teilmenge von Ω definiert. Umfasst das Ereignis genau ein Element der Ergebnismenge, handelt es sich um ein Elementarereignis. Zusammengesetzte Ereignisse beinhalten mehrere Ergebnisse. Das Ergebnis ist also ein Element der Ergebnismenge, das Ereignis jedoch eine Teilmenge, wobei diese Unterscheidung häufig vernachlässigt wird. Damit man den Ereignissen in sinnvoller Weise Wahrscheinlichkeiten zuordnen kann, werden sie in einem Mengensystem aufgeführt, der Ereignisalgebra oder

dem *Ereignisraum* Σ, eine Menge von Teilmengen von Ω. Die Wahrscheinlichkeiten ergeben sich dann als Abbildung P des Ereignisraums in das Intervall [0,1] als *Wahrscheinlichkeitsmaß*. Das Wahrscheinlichkeitsmaß ist ein *Maß P:* $\Sigma \rightarrow [0,1]$ im Sinne der Maßtheorie mit $P(\Omega)=1$.



Beispiel: Zwei Glücksräder und ihre Wahrscheinlichkeitsräume

Das Tripel (Ω, Σ, P) wird als *Wahrscheinlichkeitsraum* bezeichnet.

In dem typischen Fall, dass der Wahrscheinlichkeitsraum aus den reellen Zahlen besteht, muss bezüglich der Zuordnung der Wahrscheinlichkeiten zu den Ereignissen zwischen einer abzählbaren und überabzählbaren Ergebnismenge unterschieden werden.

Bei einer abzählbaren Ergebnismenge kann jedem Elementarereignis eine positive Wahrscheinlichkeit zugewiesen werden. Wenn Ω endlich oder abzählbar ist, kann man für die σ-Algebra Σ die Potenzmenge von Ω wählen. Die Summe der Wahrscheinlichkeiten aller Elementarereignisse aus Ω ist hier 1.

Ein Prototyp einer überabzählbaren Ergebnismenge ist die Menge der reellen Zahlen. In vielen Modellen ist es nicht möglich, *allen* Teilmengen der reellen Zahlen sinnvoll eine Wahrscheinlichkeit zuzuordnen. Als Ereignissystem wählt man statt der Potenzmenge der reellen Zahlen hier meist die Borelsche σ-Algebra, das ist die kleinste σ-Algebra, die alle Intervalle von reellen Zahlen als Elemente enthält. Die Elemente dieser σ-Algebra nennt man Borelsche Mengen oder auch (Borel)-meßbar. Wenn die Wahrscheinlichkeit $P(A)$ jeder Borelschen Menge A als Integral

$$P(A) = \int_A f(x)\,dx$$

über eine Wahrscheinlichkeitsdichte f geschrieben werden kann, wird P absolut stetig genannt. In diesem Fall (aber nicht nur in diesem) haben alle Elementarereignisse {x} die Wahrscheinlichkeit 0. Die Wahrscheinlichkeitsdichte eines absolut stetigen Wahrscheinlichkeitsmaßes P ist nur fast überall eindeutig bestimmt, d. h. sie kann auf einer beliebigen Lebesgue-Nullmenge, also einer Menge vom Lebesgue-Maß 0 abgeändert werden, ohne daß P verändert wird. Wenn die erste Ableitung der Verteilungsfunktion von P existiert,

so ist sie eine Wahrscheinlichkeitsdichte von P. Die Werte der Wahrscheinlichkeitsdichte werden jedoch nicht als Wahrscheinlichkeiten interpretiert.

Im Rahmen eines maßtheoretischen Aufbaus der Wahrscheinlichkeitstheorie wird der Begriff der Wahrscheinlichkeitsdichte verallgemeinert zum Begriff der Dichte eines Wahrscheinlichkeitsmaßes relativ zu einem Referenzmaß. Im oben beschriebenen Fall ist das Referenzmaß gleich dem Borel-Lebesgue-Maß.

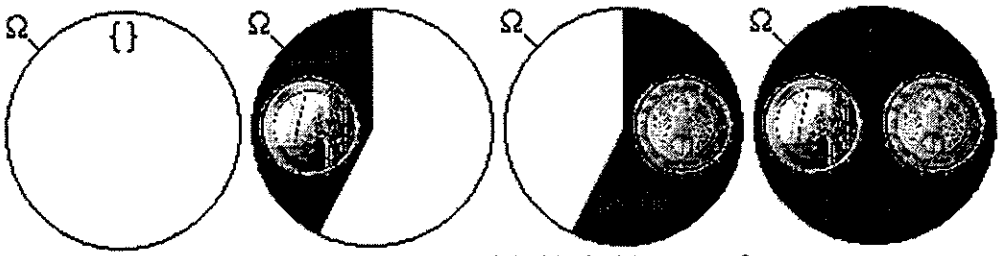
Axiome von Kolmogorow

Die axiomatische Begründung der Wahrscheinlichkeitstheorie wurde in den 1930er Jahren von Andrei Kolmogorow entwickelt. Ein Wahrscheinlichkeitsmaß wird durch die folgenden drei Kolmogorow-Axiome definiert:

1. Für jedes Ereignis A aus Ω ist die Wahrscheinlichkeit eine reelle Zahl zwischen 0 und 1: $0 \leqslant P(A) \leqslant 1$.
2. Das sichere Ereignis hat die Wahrscheinlichkeit 1: $P(\Omega)=1$.
3. Die Wahrscheinlichkeit einer Vereinigung abzählbar vieler *inkompatibler* Ereignisse entspricht der Summe der Wahrscheinlichkeiten der einzelnen Ereignisse. *Inkompatible Ereignisse* sind disjunkte Mengen A_1, A_2 ...; es muss gelten: $P(A_1 \dot{\cup} A_2 \dot{\cup} \cdots) = \sum P(A_i)$. Diese Eigenschaft wird auch σ-Additivität genannt.

Beispiel: Die Ereignisse beim Werfen einer Münze mögen *Zahl* oder *Adler* lauten.

- Dann ist die *Ergebnis*menge $\Omega=\{\text{Zahl},\text{Adler}\}$.
- Die *Ereignis*menge ist die Potenzmenge $\Pi(\Omega)$, also $\Sigma=\{\{\},\{\text{Zahl}\},\{\text{Adler}\},\Omega\}$.
- Für das Wahrscheinlichkeitsmaß P steht aufgrund der Axiome fest:
  - $P(\{\}) = 0$;
  - $P(\{Zahl\}) = 1 - P(\{Adler\})$;
  - $P(\Omega) = 1$.



Ergebnismenge und Teilmengen bei einem (nicht idealen) Münzwurf

Zusätzliches (außermathematisches) Wissen ist erforderlich, um $P(\{Zahl\}) = P(\{Adler\}) = 0{,}5$ anzusetzen. Dies kann ja durchaus von der Beschaffenheit der Münze abhängen.

Folgerungen

Aus den Axiomen ergeben sich unmittelbar einige Folgerungen:

1. Aus der Additivität der Wahrscheinlichkeit disjunkter Ereignisse folgt, dass komplementäre Ereignisse komplementäre Wahrscheinlichkeiten haben: $P(\Omega \backslash A) = 1\text{-}P(A)$.

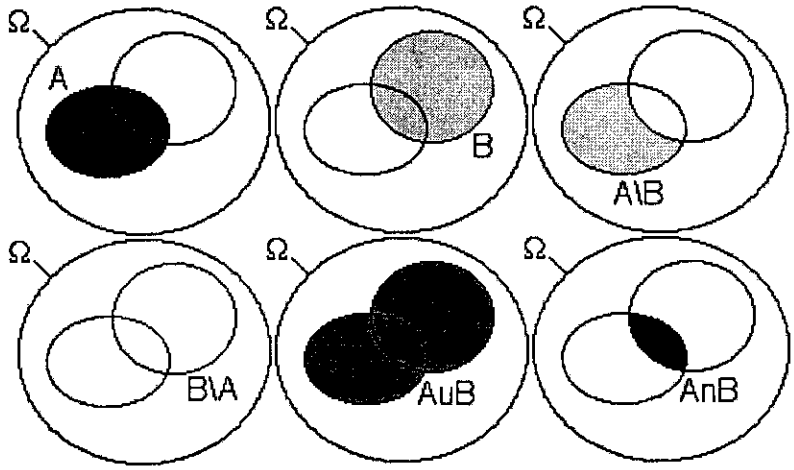
Beweis: Es ist $(\Omega \setminus A) \cup A = \Omega$ sowie $(\Omega \setminus A) \cap A = \{\}$. Folglich nach Axiom (3):

$P(\Omega \setminus A) + P(A) = P(\Omega)$ und dann nach Axiom (2): $P(\Omega \setminus A) + P(A) = 1$.
Umgestellt ergibt sich: $P(\Omega \setminus A) = 1 - P(A)$, wie behauptet.

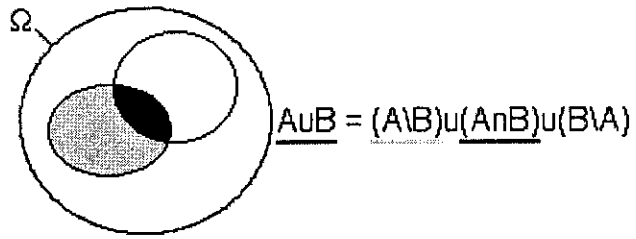
2. Daraus folgt unmittelbar, dass das *unmögliche Ereignis,* die leere Menge, die Wahrscheinlichkeit Null hat: $P(\{\})=0$.

Beweis: Es ist $\{\} \cup \Omega = \Omega$ und $\{\} \cap \Omega = \{\}$, also nach Axiom (3): $P(\{\}) + P(\Omega) = P(\Omega)$, d. h. nach Axiom (2): $P(\{\}) + 1 = 1$. Hieraus folgt $P(\{\}) = 0$, wie behauptet.

3. Für die Vereinigung nicht notwendig disjunkter Ereignisse folgt:
$P(A \cup B) = P(A) + P(B) - P(A \cap B)$.



Beweis: Die für den Beweis erforderlichen Mengen sind im obigen Bild dargestellt. Die Menge $A \cup B$ kann danach als Vereinigung von drei disjunkten Mengen dargestellt werden:



Hieraus folgt nach (3): $P(A \cup B) = P(A \setminus B) + P(A \cap B) + P(B \setminus A)$.
Andererseits ist nach (3) sowohl
$P(A) = P(A \setminus B) + P(A \cap B)$ als auch
$P(B) = P(A \cap B) + P(B \setminus A)$.
Addition liefert:
$P(A) + P(B) = P(A \setminus B) + P(A \cap B) + P(A \cap B) + P(B \setminus A)$
$= P(A \cup B) + P(A \cap B)$.
Umstellen ergibt $P(A \cup B) = P(A) + P(B) - P(A \cap B)$, wie behauptet.

Die Siebformel von Poincaré-Sylvester verallgemeinert diese Behauptung im Falle *n* verschiedener (nicht notwendig disjunkter) Teilmengen.

Spezielle Eigenschaften im Fall diskreter Wahrscheinlichkeitsräume

Laplace-Experimente

Wenn man annimmt, dass nur endlich viele Elementarereignisse möglich sind und alle gleichberechtigt sind, d. h. mit der gleichen Wahrscheinlichkeit eintreten (wie zum Beispiel beim Werfen einer idealen Münze {*Zahl*} und {*Adler*} jeweils die Wahrscheinlichkeit 0,5 besitzen), so spricht man von einem Laplace-Experiment. Dann lassen sich Wahrscheinlichkeiten einfach berechnen: Wir nehmen eine endliche Ergebnismenge Ω an, die die Mächtigkeit $|\Omega| = n$ besitzt, d. h. sie hat n Elemente. Dann ist die Wahrscheinlichkeit jedes Elementarereignisses einfach $P = \frac{1}{n}$.

Beweis: Wenn $|\Omega| = n$ ist, dann gibt es n Elementarereignisse E_1 bis E_n. Es ist dann einerseits $\Omega = E_1 \cup \ldots \cup E_n$ und andererseits sind je zwei Elementarereignisse disjunkt (inkompatibel: wenn das eine eintritt, kann das andere nicht eintreten). Also sind die Voraussetzungen für Axiom (3) erfüllt, und es gilt:
$P(E_1) + \ldots + P(E_n) = P(\Omega) = 1$.

Da nun andererseits $P(E_1) = \ldots = P(E_n) = P$ sein soll, ist $n \cdot P = 1$ und daher umgestellt: $P = \frac{1}{n}$,

wie behauptet.

Als Konsequenz folgt, dass für Ereignisse, die sich aus mehreren Elementarereignissen zusammensetzen, die entsprechend vielfache Wahrscheinlichkeit gilt. Ist A ein Ereignis der Mächtigkeit $|A| = m$, so ist A die Vereinigung von m Elementarereignissen. Jedes davon hat die Wahrscheinlichkeit $P = \frac{1}{n}$, also ist $P(A) = m \cdot \frac{1}{n} = \frac{m}{n}$. Man erhält also den einfachen Zusammenhang:

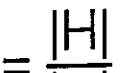
$$P(A) = \frac{|A|}{|\Omega|}.$$

Bei Laplace-Versuchen ist die Wahrscheinlichkeit eines Ereignisses gleich der Zahl der für dieses Ereignis günstigen Ergebnisse, dividiert durch die Zahl der insgesamt möglichen Ergebnisse.

Das nachstehende Bild zeigt ein Beispiel beim Würfeln mit einem idealen Würfel (Laplace-Würfel).

$\Omega = \{$  $\}$

$H = \{$  $\}$

$$P(H) = \frac{|H|}{|\Omega|} = \frac{|\{ \text{  } \}|}{|\{ \text{  } \}|} = \frac{2}{6} = \frac{1}{3}$$

Das Ereignis H = Hohe Augenzahl (5 oder 6) hat die Wahrscheinlichkeit $^1/_3$.

Ein typischer Laplace-Versuch ist auch das Ziehen einer Karte aus einem Spiel mit n Karten oder das Ziehen einer Kugel aus einer Urne mit n Kugeln. Hier hat jedes Elementarereignis die gleiche Wahrscheinlichkeit.

(2)

Elem. Math. 57 (2002) 90 – 95
0013-6018/02/030090-6

Elemente der Mathematik

Die Riemannsche Vermutung

Jürg Kramer

1 Einführung

In dem hier vorzustellenden Millenniumsproblem handelt es sich um eine zahlentheoretische Fragestellung aus dem 19. Jahrhundert, die seit ein paar Jahren auch überraschende Zusammenhänge zu anderen Gebieten der Mathematik und der theoretischen Physik erkennen lässt. Die Problemstellung hat ihren Ursprung bei der Frage nach der Dichte der Primzahlen im Bereich der natürlichen Zahlen. Um den Leser in den Problemkreis einzuführen, wollen wir einfach beginnen. Wir bezeichnen mit $\mathbb{N}$ die Menge der natürlichen Zahlen, d.h.

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}.$$

Mit $\mathbb{P}$ bezeichnen wir die Menge der Primzahlen, d.h. die Menge aller natürlichen Zahlen grösser als Eins, die nur durch sich selbst und durch Eins teilbar sind, also

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, \ldots, 229, \ldots\}.$$

Wir erinnern nun an zwei Tatsachen, die vermutlich den meisten Lesern wohl bekannt sind.

Das erste ist die Tatsache, dass jede positive natürliche Zahl n sich bis auf die Reihenfolge eindeutig als Produkt von Primzahlpotenzen darstellen lässt, d.h. es gibt Primzahlen $p_1, \ldots, p_r$ und natürliche Zahlen $\alpha_1, \ldots, \alpha_r$ derart, dass die Gleichheit

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$$

besteht. Dies ist der Inhalt des sogenannten *Fundamentalsatzes der Zahlentheorie*, der mit anderen Worten besagt, dass die Primzahlen die multiplikativen Bausteine der natürlichen Zahlen sind.

Als zweites erinnern wir an den *Satz von Euklid*, dass es nämlich unendlich viele Primzahlen gibt. Dies sieht man leicht wie folgt ein: Man nimmt im Gegenteil zur Behauptung an, dass es nur endlich viele Primzahlen $p_1, \ldots, p_N$ gibt. Damit bildet man die (sehr grosse) Zahl

$$m = p_1 \cdot \ldots \cdot p_N + 1.$$

Nun besitzt die natürliche Zahl m einerseits mindestens einen Primteiler q. Da die Zahl m andererseits bei Division durch jede der Primzahlen $p_1, \ldots, p_N$ den Rest 1 lässt, muss

$q \neq p_j$ $(j = 1, \ldots, N)$ gelten. Dies ist ein Widerspruch zu unserer Annahme und beweist somit die Unendlichkeit der Anzahl der Primzahlen.

Nach dem Satz von Euklid gibt es also beliebig grosse Primzahlen. Dieser Umstand spielt heute in der Kryptographie eine wichtige Rolle. Die gegenwärtig grösste bekannte Primzahl der Form $p = 2^n - 1$, eine sogenannte *Mersennesche Primzahl*, lautet

$$p = 2^{13\,466\,917} - 1\,;$$

sie hat mehr als 4 Mio. Stellen (siehe [10]). Würde man alle Stellen ausdrucken, so wären bei der hier gewählten Schriftgrösse mehr als 1000 A4-Seiten notwendig.

2 Die Riemannsche Zetafunktion

Für reelles oder allgemeiner komplexes $s = \sigma + it$ betrachten wir die Reihe

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \ldots \tag{1}$$

Für $t = 0$ und $\sigma > 1$ erkennen wir die aus den Grundvorlesungen der Analysis wohlbekannte konvergente Reihe, die oft als Majorante herangezogen wird; für $t = 0$ und $\sigma = 1$ erhalten wir die harmonische Reihe, welche bekanntlich divergiert, allerdings sehr langsam. Betrachtet man nun die Reihe (1) als Funktion von s, so lässt sich das folgende dazu festhalten: Die Reihe (1) konvergiert für $\operatorname{Re} s = \sigma > 1$ absolut und lokal gleichmässig und definiert dort eine holomorphe Funktion, die *Riemannsche Zetafunktion* $\zeta(s)$.

Fig. 1 Bernhard Riemann

Fig. 2 Leonhard Euler

Mit Hilfe der Poissonschen Summationsformel beweist man weiter die Funktionalgleichung

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \pi^{-(1-s)/2}\Gamma((1-s)/2)\zeta(1-s)\,; \tag{2}$$

hierbei ist $\Gamma(s)$ die Eulersche Gammafunktion. Mit der Funktionalgleichung (2) zeigt man, dass sich $\zeta(s)$ zu einer meromorphen Funktion auf die gesamte komplexe Ebene $\mathbb{C}$ mit einem Pol erster Ordnung an der Stelle $s = 1$ mit Residuum 1 fortsetzen lässt.

Diese und weitere grundlegende Eigenschaften der Riemannschen Zetafunktion werden z.B. in den Lehrbüchern [2] oder [6] dargestellt.

Die hervorragende Bedeutung der Riemannschen Zetafunktion für die Arithmetik wird durch die beiden folgenden Resultate, die bereits durch L. Euler (1707–1783) entdeckt wurden, deutlich:

(i) Die Riemannsche Zetafunktion besitzt für $\operatorname{Re} s > 1$ die sogenannte *Eulersche Produktentwicklung*, d.h.

$$\zeta(s) = \prod_{p \in \mathbb{P}} (1 - p^{-s})^{-1} .$$

Die Gültigkeit dieser Produktentwicklung sieht man unmittelbar ein, indem man den Term $(1 - p^{-s})^{-1}$ durch die geometrische Reihe $\sum_{m=0}^{\infty} p^{-ms}$ ersetzt und dann sukzessive das Produkt über alle Primzahlen bildet. Dabei erkennt man, dass das Bestehen der Eulerschen Produktentwicklung für $\zeta(s)$ gleichbedeutend zum Fundamentalsatz der Arithmetik ist.

(ii) Als zweites erkennt man, dass der Satz von Euklid über die Unendlichkeit der Menge der Primzahlen äquivalent zur Tatsache ist, dass $\zeta(s)$ an der Stelle $s = 1$ einen Pol hat. Mit Hilfe der Eulerschen Produktentwicklung ergibt sich nämlich für $s \downarrow 1$

$$\lim_{s \downarrow 1} \zeta(s) = \infty ,$$

d.h. das unendliche Produkt

$$\prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-1}}$$

divergiert, was die Unendlichkeit der Menge $\mathbb{P}$ zur Folge hat.

3 Die Primzahlfunktion

Da es also unendlich viele Primzahlen gibt, kann man versuchen, deren Dichte in der Menge der natürlichen Zahlen zu ermitteln. Dazu bezeichnen wir für positives, reelles x mit $\pi(x)$ die Anzahl der Primzahlen, die kleiner oder gleich x sind, d.h.

$$\pi(x) = \#\{p \in \mathbb{P} \mid p \leq x\} .$$

Dies definiert eine reellwertige Funktion, die sogenannte *Primzahlfunktion*. Für kleine Werte von x erkennen wir $\pi(x)$ als Treppenfunktion (siehe Fig. 3); für grosse Werte von x tritt der Treppenfunktionscharakter von $\pi(x)$ in den Hintergrund, und es scheint sich asymptotisch eine glatte Funktion zu zeigen (siehe Fig. 4). Dieses Phänomen ist im wesentlichen der Inhalt des *Primzahlsatzes*, der besagt, dass für $x \to \infty$ die Asymptotik

$$\pi(x) \sim \frac{x}{\log x}$$

besteht, welche mit Hilfe des Integrallogarithmus

$$\operatorname{Li}(x) = \int_2^{\infty} \frac{dt}{\log t}$$

noch verbessert werden kann zu

$$\pi(x) \sim \mathrm{Li}(x)$$

(siehe Fig. 3, 4). Dieser Satz wurde bereits von C.F. Gauß (1777–1855) vermutet, aber erst im Jahr 1896 durch J. Hadamard (1865–1963) und C. de la Vallée Poussin (1866–1962) vollständig bewiesen.

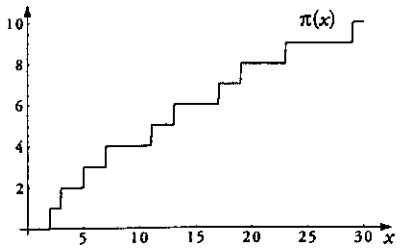


Fig. 3 Primzahlfunktion $\pi(x)$

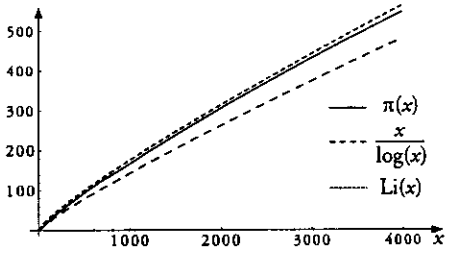


Fig. 4 Primzahlfunktion $\pi(x)$

Im Jahr 1949 fanden A. Selberg und P. Erdös (1913–1996) einen elementaren Beweis des Primzahlsatzes, der weder die Riemannsche Zetafunktion noch die Funktionentheorie verwendet (siehe [2], Chapter I). Vor kurzem, im Jahr 1997, hat D. Zagier basierend auf einer Idee von D.J. Newman einen sehr kurzen Beweis des Primzahlsatzes gegeben, der neben einigen sehr elementaren arithmetischen Tatsachen nur den Cauchyschen Integralsatz heranzieht (siehe [9]).

Nach dem Primzahlsatz besteht also für die Primzahlverteilung die Formel

$$\pi(x) = \mathrm{Li}(x) + R(x)$$

mit einem Restglied $R(x)$, welches

$$\frac{R(x)}{\mathrm{Li}(x)} \underset{x\to\infty}{\longrightarrow} 0$$

erfüllt. Nunmehr ist es natürlich von Interesse, das Restglied $R(x)$ in den Griff zu bekommen. Dies führt uns endlich zu dem in diesem Beitrag vorzustellenden Millenniumsproblem.

Riemannsche Vermutung: Diese Vermutung besagt, dass das Restglied $R(x)$ für $x \to \infty$ von der Grössenordnung

$$R(x) = O(\sqrt{x}\log x)$$

ist.

Bis heute ist man noch weit davon entfernt, diese Vermutung beweisen zu können. Noch immer ist E. Littlewoods (1885–1977) Abschätzung aus dem Jahre 1922 im wesentlichen unübertroffen. Seine Abschätzung für das Restglied $R(x)$ lautet

$$R(x) = O\left(x \cdot e^{-C\sqrt{\log x \log\log x}}\right)$$

mit einer positiven Konstanten C (siehe [2], Chapter III). Mit Hilfe der sogenannten „Expliziten Formeln" der analytischen Zahlentheorie lässt sich die Riemannsche Vermutung als Vermutung über die Lage der Nullstellen von $\zeta(s)$ umformulieren. In dieser Form hat B. Riemann (1826–1866) seine Vermutung ursprünglich festgehalten.

Äquivalente Formulierung der Riemannschen Vermutung: Abgesehen von den sogenannten „trivialen" Nullstellen der Riemannschen Zetafunktion bei $s = -2, -4, -6, -8, \ldots$ befinden sich sämtliche weiteren Nullstellen von $\zeta(s)$ auf der *kritischen Geraden* $\{s \in \mathbb{C} \mid \mathrm{Re}\, s = 1/2\}$.

Man findet die Original-Formulierung von Riemanns Vermutung in seinem Beitrag „Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse" in den Monatsberichten der Berliner Akademie vom November 1859 (siehe [8], p. 180). Nach Einführung der Funktion

$$\xi(t) = \pi^{-s(t)/2}\Gamma(s(t)/2)(s(t) - 1)\zeta(s(t))$$

mit $s(t) = 1/2 + it$ bemerkt Riemann dort: „Man findet nun in der That etwa soviele reelle Wurzeln innerhalb dieser Grenzen, und es ist sehr wahrscheinlich, dass alle Wurzeln reell sind."

4 Beweisansätze

4.1 Klassische Ergebnisse. Zunächst weist man mit verhältnismässig elementaren Mitteln nach, dass die nicht-trivialen Nullstellen von $\zeta(s)$ im *kritischen Streifen* $\{s \in \mathbb{C} \mid 0 \leq \mathrm{Re}\, s \leq 1\}$ liegen. Bezeichnet nun $N(T)$ die Anzahl der Nullstellen $s = \sigma + it$ im kritischen Streifen mit $0 \leq t \leq T$, so war bereits Riemann die Asymptotik

$$N(T) \sim \frac{T}{2\pi} \log\left(\frac{T}{2\pi}\right) \qquad (T \to \infty)$$

bekannt, welche ihn zu seiner Vermutung führte, da er experimentell in etwa ebenso viele Nullstellen auf der kritischen Geraden fand. Einen wichtigen Beitrag zur Eingrenzung der Nullstellen innerhalb des kritischen Streifens gelang E. Littlewood im Jahr 1922; allerdings ist man damit noch weit von einem Beweis der Riemannschen Vermutung entfernt. In den Folgejahren wurden im Zuge der Verbesserung der Computertechnik vermehrt numerische Experimente zur Verifikation der Riemannschen Vermutung durchgeführt. In diesem Zusammenhang sind die eindrücklichen Ergebnisse von A. Odlyzko zu erwähnen, der gegenwärtig in der Grössenordnung von 10^{22} Nullstellen der Zetafunktion auf der kritischen Geraden berechnet hat (siehe [7]).

4.2 Ältere und neuere Bezüge. Die Riemannsche Vermutung hat E. Artin (1898–1962) und A. Weil (1906–1998) zu analogen Vermutungen zur Kongruenzzetafunktion algebraischer Varietäten über endlichen Körpern veranlasst. Beginnend mit den Resultaten von H. Hasse (1898–1979) in den 30er Jahren wurden diese Vermutungen in den 70er Jahren durch P. Deligne vollständig bewiesen, was als Evidenz für die Gültigkeit der Riemannschen Vermutung gewertet werden kann.

Die neuesten Entwicklungen zielen darauf ab, die Nullstellen von $\zeta(s)$ bzw. $\xi(t)$ als Eigenwerte eines unendlich dimensionalen Operators zu deuten, um dann die Riemannsche

Vermutung mit Hilfe geeigneter kohomologischer Methoden (wie im Fall der Kongruenzzetafunktion) zu beweisen; diese Idee geht bereits auf D. Hilbert (1862–1943) zurück (siehe [4]). Eine weitere, überraschende Entdeckung von C. Deninger bringt die bereits erwähnten „Expliziten Formeln" mit der Theorie gewisser dynamischer Systeme in Zusammenhang (siehe [5]). Schliesslich verweisen wir auf die ebenso überraschenden Verbindungen zur Physik, genauer zu chaotischen, quantenmechanischen Sytemen (siehe [3]).

Literatur

[1] Bombieri, E.: Problems of the Millennium: The Riemann Hypothesis. pdf-file unter http://www.claymath.org/prizeproblems/riemann.htm

[2] Chandrasekharan, K.: *Arithmetical functions*. Grundlehren der math. Wiss. 167. Springer-Verlag. Berlin, Heidelberg, New York 1970.

[3] Cipra, B.: *A prime case of chaos*. In: What's happening in the mathematical sciences. Vol. 4, AMS, 1999.

[4] Connes, A.: Trace formula in noncommutative geometry and the zeros of the Riemann zeta function. *Selecta Math.* 5 (1999), 29–106.

[5] Deninger, C.: *Some analogies between number theory and dynamical systems on foliated spaces*. Proc. Int. Congr. Math., vol. I, 163–186. Berlin 1998.

[6] Edwards, H.M.: *Riemann's zeta function*. Academic Press. New York, London 1974.

[7] Odlyzko, A.: Tables of zeros of the Riemann zeta function. http://www.dtc.umn.edu/~odlyzko/zeta_tables/index.html

[8] Riemann, B.: *Gesammelte mathematische Werke, wissenschaftlicher Nachlass und Nachträge, Collected Papers*. Springer-Verlag/B.G. Teubner Verlagsgesellschaft. Berlin, Heidelberg/Leipzig 1990.

[9] Zagier, D.: Newman's short proof of the prime number theorem. *Am. Math. Mon.* 104 (1997), 705–708.

[10] http://www.mersenne.org/prime.htm

Jürg Kramer
Institut für Mathematik
Humboldt-Universität zu Berlin
D–10099 Berlin
e-mail: kramer@mathematik.hu-berlin.de

Grundbegriffe

Aussagen sind dabei Folgen von Zeichen, die ähnlich wie ein Programm einer Programmiersprache einer gewissen Syntax genügen müssen und die mittels einer Semantik eine Bedeutung erhalten und sich dadurch in wahre und falsche Aussagen unterteilen lassen (wobei zu einer gegebenen Aussage nicht notwendigerweise sofort klar ist, ob sie wahr oder falsch ist), siehe Formales System. Für gewöhnlich lassen sich dabei zu einer Aussage auch leicht komplementäre Aussagen derart konstruieren, dass entweder die Aussage selbst oder die komplementäre Aussage wahr ist, aber niemals beide zugleich.

Die Aufgabe einer formalen Theorie ist es dann, aus bestimmten Grundaussagen (Axiomen), die generell als *wahr* angenommen werden, über allgemein akzeptierte Ableitungsregeln weitere wahre Aussagen abzuleiten. Eine Folge solcher Ableitungen nennt man dann **Beweis** der entsprechenden abgeleiteten Aussage, da sie die Allgemeingültigkeit der Aussage zeigt (siehe Gödelscher Vollständigkeitssatz). Im Idealfall wünscht man sich, dass aus der Menge der Grundaussagen und den Ableitungsregeln alle wahren Aussagen abgeleitet, also bewiesen werden können. Ein derartiges System nennt man dann **vollständig** (andernfalls **unvollständig**). Eine formale Theorie sollte zudem auch **widerspruchsfrei** sein, das heißt es lassen sich keine falschen Aussagen ableiten. Genauer formuliert, lassen sich nicht gleichzeitig eine Aussage und eine dazu (im obigen Sinne) komplementäre Aussage ableiten. Eine formale Theorie, die dem nicht genügt, nennt man **widersprüchlich**.

Gödels Satz

Der Mathematiker Kurt Gödel wies im Jahre 1930 nach, dass man in Systemen wie der Arithmetik nicht alle Aussagen formal beweisen oder widerlegen kann. Sein Satz besagt:

Jedes hinreichend mächtige formale System ist entweder widersprüchlich oder unvollständig.

Gödels Argumentation läuft auf eine Abzählung aller Sätze innerhalb des formalen Systems hinaus, jeder Satz erhält eine eigene Nummer. Er konstruiert dann eine Aussage der Form: "*Der Satz mit der Nummer x ist nicht ableitbar*" und zeigt, dass es eine Einsetzung für *x* gibt so dass *x* die Nummer dieser Aussage ist. Insgesamt erhält er einen Satz der Form "*Ich bin nicht ableitbar*". Es gibt nun zwei Möglichkeiten: Entweder dieser "*Satz x*" ist wahr, dann ist er nicht ableitbar (genau das ist sein Inhalt: Ich bin nicht ableitbar!). Oder "*Satz x*" ist falsch, dann muss der Satz ableitbar sein und demnach wahr sein. Das ist ein Widerspruch; also kann dieser Satz nur falsch sein, wenn das formale System widersprüchlich ist oder wahr, wenn das formale System unvollständig ist.

Man beachte: Der Satz mit Nummer *x* und der Bedeutung "*Satz x ist nicht ableitbar*", ist damit bewiesen: Wir vertrauen auf diesen Beweis, obwohl es innerhalb des Systems keine Ableitung gibt!

Damit obiger Ansatz funktioniert, muss das zugrundegelegte formale System also mindestens Zählungen und eine Multiplikation mit einer Konstanten größer als 1 (für Kodierungszwecke) erlauben. Für zu einfache Systeme gilt der Unvollständigkeitssatz daher nicht. Die Möglichkeit von Addition und Multiplikation sind ganz wesentliche Eigenschaften in vielen Theorien, so dass hier dieser Satz gilt.

Normalerweise könnte man sich dadurch behelfen, dass man für alle Sätze, die weder bewiesen noch widerlegt werden können, einfach definiert, ob sie als wahr oder falsch gelten und die Definition dem formalen System hinzufügt. Im neuen, erweiterten System existiert dann für diese Sätze ein Beweis, nämlich einfach die hinzugefügte Definition. Lesen wir jedoch erneut den Satz, den Gödel bewiesen hat, so sehen wir, dass auch hier die Voraussetzungen erfüllt sind und somit auch das erweiterte System unvollständig bleibt, da stets unbeweisbare Sätze übrigbleiben.

Bedeutung des Unvollständigkeitssatzes

Gödel versetzte mit seinem Unvollständigkeitssatz einem Ansatz von David Hilbert zur vollständigen Begründung und Formalisierung der Mathematik einen schweren Schlag. Dieser Ansatz ist als Hilberts Programm bekannt geworden und wurde von ihm im Jahre 1921 veröffentlicht. Hilbert schlug vor, die Widerspruchsfreiheit von komplexeren Systemen durch einfachere Systeme nachzuweisen. Hintergrund ist der, dass einem Beweis zur Widerspruchsfreiheit eines Systems, der in diesem System selbst gegeben ist, nicht getraut werden kann. Der Grund ist, dass sich aus einem Widerspruch heraus alles beweisen lässt (Ex falso quodlibet), also ließe sich aus einem Widerspruch im System auch die Widerspruchsfreiheit des Systems beweisen. Daher sollte die Widerspruchsfreiheit in einem einfacheren System bewiesen werden.

Eine streng formalisierte Prädikatenlogik erster Stufe war eines von Hilberts Konzepten. Am Ende seines Programms sollte die gesamte Mathematik auf die einfache Arithmetik zurückgeführt und auf ein axiomatisches System gestellt werden, aus dem alle mathematischen Sätze streng ableitbar sind.

Gödels Arbeit war durch Hilberts Programm motiviert. Er verwendete die von Hilbert vorgeschlagenen Methoden, um seinen Unvollständigkeitssatz zu zeigen. Gödel bewies auch den folgenden Satz

Ein System kann nicht zum Beweis seiner eigenen Widerspruchsfreiheit verwendet werden.

Gödel hatte damit gewissermaßen Hilbert mit dessen Methoden gezeigt, dass der Vorschlag nicht funktioniert.

Die Folge daraus ist, dass man die Korrektheit von (gewissen) formalen Systemen *als gegeben annehmen* muss, sie lassen sich nicht beweisen.

Ein anderer Ansatz, der unüberbrückbare Lücken in Hilberts Programm nachweist, stammt von dem

Mathematiker Alan Turing. Er erfand die *Turingmaschine* und formulierte deren Halteproblem.

Genauere Formulierung

Der Gödelsche Satz besagt genauer, dass jedes Beweissystem für die Menge der wahren arithmetischen Formeln unvollständig ist (sofern man voraussetzt, dass die Arithmetik widerspruchsfrei ist - was, wie Gödel auch zeigt, nicht mit Mitteln der untersuchten Theorie allein bewiesen werden kann). Das heißt:

In jeder formalen Theorie, welche mindestens so mächtig wie die Theorie der natürlichen Zahlen (Peano-Arithmetik) ist, bleiben wahre (und falsche) arithmetische Formeln übrig, die nicht innerhalb der Theorie beweisbar (widerlegbar) sind. Paul Cohen bewies 1963, dass sowohl das Auswahlaxiom als auch die Kontinuumshypothese auf Grundlage der Zermelo-Fraenkel-Mengenlehre formal unentscheidbar sind. Er fand damit die ersten Beispiele mathematisch bedeutsamer unentscheidbarer Sätze, deren Existenz Gödel bewiesen hatte.

Damit eine Theorie (in der Prädikatenlogik erster Stufe, PL1) die Voraussetzungen für die Unvollständigkeit erfüllt, muss gelten:

- Zu jeder durch einen Ausdruck G(x) beschriebenen Menge ist das Komplement beschreibbar.
- Zu jeder durch einen Ausdruck G(x) beschriebenen Menge M ist die Menge $M^*=\{x|d(x)\in M\}$ beschreibbar; Dabei ist d(x) die Diagonalisierung von x.
- Die Menge der beweisbaren Ausdrücke der Theorie ist durch einen Ausdruck der Form G(x) beschreibbar.

Nach dem Satz von Löwenheim-Skolem findet man zu jeder Theorie in PL1 ein Modell mit der Mächtigkeit der Signatur. Für "normale" Theorien existiert also ein abzählbares Modell, beispielsweise die natürlichen Zahlen (das heißt es lässt sich für jede Theorie in PL1 auch ein Modell finden, in dem die Objekte natürliche Zahlen sind). Die Idee von Gödel war, Formeln der Theorie selbst zum Objekt derselben zu machen. Dazu wurden die Formeln gödelisiert, das heißt eine (bijektive) Abbildung von Formeln auf natürliche Zahlen gebildet. Das kann man zum Beispiel dadurch erreichen, dass jedem Symbol der Signatur eine Zahl zugeordnet wird, die dann verkettet werden. Ordnet man der **0** die *1* und = die *2* zu, so ist die Gödelnummer der Formel (in dem Spezialfall) **0=0** die *121*. Die Verkettungsoperation ist einfach durch Exponentieren zu realisieren. Es lassen sich auch die syntaktisch wohlgeformten, und schließlich die beweisbaren Formeln durch arithmetische Ausdrücke (Addition, Multiplikation, Exponentiation) beschreiben.

Die Diagonalisierung in Gödels Beweis ist nun eine Anwendung eines Ausdrucks P(x) auf die eigene Gödelnummer. Ist die Gödelnummer des Ausdrucks (und damit der Zeichenreihe) P(x) zum Beispiel **12345**, so ist die Diagonalisierung der Zahl **12345** die Gödelnummer von **P(12345)** (selbstverständlich hat eine Zahl, hier **12345**, auch eine Gödelnummer, die entsteht, indem man alle vorkommenden Ziffern gödelisiert).

"Besagt" der Ausdruck **B(x)** also, dass **x** ableitbar ist, und ist zum Beispiel **12345** die Gödelnummer von **B(x)**, so ist ¬B(12345) eine nicht ableitbare Aussage. Diese Aussage besagt dann nämlich: Die Formel mit der Gödelnummer **12345** ist nicht ableitbar. **12345** ist aber die Gödelnummer von B(x). Also sagt ¬B(12345): Ich bin nicht ableitbar. Wenn PA korrekt ist, so ist dieser Satz wahr (in PA), aber nicht ableitbar.

Gödels ursprünglicher Beweis ging noch weiter. Er wollte Rückgriffe auf die Semantik, insbesondere die Korrektheit, vermeiden. Deswegen bewies er seinen Unvollständigkeitssatz unter der Voraussetzung der ω-Konsistenz: Eine Theorie ist ω-inkonsistent, wenn ein Ausdruck mit einer einzigen freien Variable x existiert, für den $\exists x P(x)$ ableitbar ist, zugleich aber für alle $n < \omega$ $\neg P(n)$ ableitbar ist.

Rosser erweiterte das Gödelsche Resultat, indem er einen Unvollständigkeitsbeweis lieferte, für den nicht die

Menge der Ausdrücke, deren Diagonalisierung beweisbar ist, beschrieben wird, sondern eine zu dieser Menge disjunkte Obermenge der Ausdrücke, deren Diagonalisierung widerlegbar ist. Dadurch ist auch der Bezug auf die ω-Konsistenz überflüssig.

Gödels zweiter Unvollständigkeitssatz ist eine leicht zu sehende Konsequenz aus dem ersten. Da Gödel beweisbare Aussagen innerhalb der Prädikatenlogik formalisierte (beispielsweise durch das Prädikat $B(x)$), lässt sich auch folgende Aussage bilden: $\neg B(\bot)$, wobei $\bot$ die Gödelnummer von einer beliebigen Kontradiktion, zum Beispiel $\neg 0 = 0$, ist. Die Aussage $W = \neg B(\bot)$ "behauptet" die Nichtbeweisbarkeit einer Kontradiktion, und damit die Widerspruchsfreiheit der gesamten Theorie (der Peano-Arithmetik). W ist in PA nicht beweisbar. Um die Nicht-Beweisbarkeit zu zeigen, wird eine Fixpunktkonstruktion verwendet. Sei $g(x)$ die Gödelisierungsfunktion, A eine Aussage, $B(x)$ ein Prädikat. A heißt Fixpunkt für $B(x)$, wenn $A \iff B(g(A))$ beweisbar ist. Über einfache aussagenlogische Konstruktionen lässt sich beweisen, dass $W \rightarrow A$ beweisbar ist, wenn A Fixpunkt von $\neg B(x)$ ist. Außerdem kann leicht gezeigt werden, dass, wenn A Fixpunkt von $\neg B(x)$ ist, A nicht beweisbar ist, falls PA konsistent ist. Daraus folgt dann, dass W nicht beweisbar ist.

Durch diese erstaunlichen Sätze ist der Mathematik eine prinzipielle Grenze gesetzt: Nicht jeder wahre mathematische Satz kann aus den wie auch immer gewählten Axiomen eines mathematischen Teilgebietes (zum Beispiel Arithmetik, Geometrie, Algebra etcetera) formal abgeleitet werden.

Viel Verwirrung entsteht aus dem Zusammenhang der Gödelschen Unvollständigkeitssätze mit dem Gödelschen Vollständigkeitssatz. Der Gödelsche Vollständigkeitssatz besagt, dass in der Prädikatenlogik erster Stufe (PL1) alle ableitbaren Sätze wahr, und umgekehrt alle wahren Sätze ableitbar sind, und damit, dass Syntax und Semantik für die PL1 zusammenfallen.

Im Gegensatz dazu wird in den Unvollständigkeitssätzen bereits ein Modell betrachtet, die Struktur der natürlichen Zahlen, die Peano-Arithmetik. Die Unvollständigkeitssätze sagen dann aus, dass in diesem Modell wahre Sätze existieren, die in der Prädikatenlogik erster Stufe nicht abgeleitet werden können. Da sie wahr sind in PA, zeigt dies auch, dass die Peano-Arithmetik nicht in PL1 (bis auf Isomorphie) formalisiert werden kann.

Interessantes

Gödel nannte seinen Aufsatz *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*, weil er plante, einen zweiten Aufsatz zu verfassen, in dem er den Beweis genauer erläutern wollte. Der erste Aufsatz fand jedoch bereits so große Anerkennung, dass der Bedarf für einen zweiten entfiel, der daher auch nie geschrieben wurde.

Konkret bezog sich Gödels Aufsatz auf die Principia Mathematica, ein großes formales System, das Bertrand Russell und Alfred North Whitehead zwischen 1910 und 1913 veröffentlichten. Gödel zeigte jedoch auf, dass jedes System mit der gleichen Mächtigkeit wie die Principia Mathematica ebenso anfällig ist.

Weiterhin konnte Gerhard Gentzen zeigen, dass eine konstruktive Mathematik und Logik durchaus widerspruchsfrei ist. Hier zeigt sich ein Grundlagenstreit der Mathematik. Der Philosoph Paul Lorenzen hat eine widerspruchsfreie Logik und Mathematik erarbeitet (Methodischer Konstruktivismus), und sein Buch Metamathematik (1962) eigens geschrieben, um zu zeigen, dass der Gödelsche Unvollständigkeitssatz keinen Einwand gegen einen widerspruchsfreien Aufbau der Mathematik darstellt.

Eine interessante und relativ leicht verständliche Erklärung von Gödels Satz und seinen Implikationen gibt das Buch "Gödel, Escher, Bach" von Douglas Hofstadter.