Primzahlen und Chaos

Jürg Kramer

Institut für Mathematik
Humboldt-Universität zu Berlin

24. April 2008

Die natürlichen Zahlen

- Die Menge der natürlichen Zahlen:

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

- Die Menge der ganzen Zahlen:

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

Operationen

- Addition $+$

$$n, m \in \mathbb{Z} \Longrightarrow n+m \in \mathbb{Z}$$

- Multiplikation $\bullet$

$$n, m \in \mathbb{Z} \Longrightarrow n \bullet m \in \mathbb{Z}$$

- Gesetze

$n+m = m+n$	Kommutativität von $+$
$n \bullet m = m \bullet n$	Kommutativität von $\bullet$
$n+(m+k) = (n+m)+k$	Assoziativität von $+$
$n \bullet (m \bullet k) = (n \bullet m) \bullet k$	Assoziativität von $\bullet$
$n \bullet (m+k) = n \bullet m + n \bullet k$	Distributiviät von $+$ und $\bullet$

Bausteine

- Alle natürlichen Zahlen lassen sich als Summe von Einsen darstellen, z.B.

$$5 = 1 + 1 + 1 + 1 + 1$$

- Die Zahl 1 ist der additive Baustein.
- Multiplikative Bausteine?

Primzahlen

Definition

Eine natürliche Zahl p heißt Primzahl, falls $p > 1$ ist und nur die Teiler 1 und p hat.

- Fundamentalsatz der Arithmetik
  Alle natürlichen Zahlen lassen sich (bis auf die Reihenfolge eindeutig) als Produkt von Primzahlen darstellen, z.B.

$$96 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^5 \cdot 3$$

- Die Primzahlen sind die multiplikativen Bausteine.

Sieb des Eratosthenes

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Sieb des Eratosthenes

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Sieb des Eratosthenes

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Sieb des Eratosthenes

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Sieb des Eratosthenes

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Sieb des Eratosthenes

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Wie viele Primzahlen gibt es?

Theorem (Euklid)

Es gibt unendlich viele Primzahlen.

Beweis.

- Annahme:
  Es gibt nur endlich viele Primzahlen $p_1, p_2, \ldots, p_n$.
- Sei $q = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ das Produkt dieser Primzahlen.
- Die Zahl $q + 1$ ist durch keine der Primzahlen p_i teilbar, da bei Division durch p_i immer der Rest 1 bleibt.
- Damit sind die Primfaktoren von $q + 1$ nicht in der Menge der Primzahlen $p_1, p_2, \ldots, p_n$ enthalten.
- Dies widerspricht unserer Annahme.

Mersenne'sche Primzahlen

Dies sind Primzahlen der Form

$$p = 2^n - 1,$$

wobei notwendigerweise n selbst auch eine Primzahl ist.

- $n = 2$: $\quad 2^2 - 1 = 3$
- $n = 3$: $\quad 2^3 - 1 = 7$
- $n = 5$: $\quad 2^5 - 1 = 31$
- Gegenbeispiel: $2^{11} - 1 = 2047 = 23 \cdot 89$

Fermat'sche Primzahlen

Dies sind Primzahlen der Form
$p = 2^n + 1$,
wobei notwendigerweise $n = 2^m$
mit $m \in \mathbb{N}$ ist.

- $n = 2^0$: $\quad p = 2^1 + 1 = 3$
- $n = 2^1$: $\quad p = 2^2 + 1 = 5$
- $n = 2^2$: $\quad p = 2^4 + 1 = 17$
- $n = 2^3$: $\quad p = 2^8 + 1 = 257$
- $n = 2^4$: $\quad p = 2^{16} + 1 = 65\,537$
- Gegenbeispiel (Euler):
  $p = 2^{2^5} + 1 = 4\,294\,967\,297$ hat den Teiler 641

Primzahlen und Chaos

Jürg Kramer

Natürliche Zahlen
Bausteine
Primzahlen
Sieb des Eratosthenes
Euklid
Formeln für Primzahlen
Anwendung
Zählen von Primzahlen
Riemannsche Vermutung
Riemannsche Zetafunktion
Klassische Mechanik
Quantenmechanik

Größte bekannte Primzahl

- Die derzeit größte bekannte Primzahl (Stand: 04.09.2006)

$$p = 2^{32\,582\,657} - 1$$

- Dies ist eine Zahl mit 9 808 358 Stellen.
- http://primes.utm.edu/largest.html
- Etwa 2500 eng bedruckte DIN-A4 Seiten, beginnend mit
  1245750260153694554008555015747995031227959851511
  5184284367047566259111523599739738055975960661684
  5939100419886882111308706204284904304856342719392
  4179676463175953389304422007303179021122683590423
  0987323393908925421059845352243092506329878772608
  4980682705539089064014845620373601193375780239969
  2661758862749761713589606175375030205627843573215 . . .

Anwendung

Primzahlen und ihre Eigenschaften finden Anwendung bei:

- Verwendung von EC-Karten
- Sicheres Kommunizieren
- Verwendung des Internets
- ...

Anwendung

Wichtiges Instrument: Kleiner Satz von Fermat

$$R_p(a^p) = a \Longleftrightarrow R_p(a^{p-1}) = 1$$

$$(p \text{ Primzahl}, \ 0 < a < p)$$

$R_p(b) =$ Rest von b nach Division durch p

Anwendung

Wichtiges Instrument: Kleiner Satz von Fermat

$$R_p(a^p) = a \Longleftrightarrow R_p(a^{p-1}) = 1$$

$$(p \text{ Primzahl, } 0 < a < p)$$

$R_p(b) =$ Rest von b nach Division durch p

- $R_5(2^1) = 2,\ R_5(2^2) = 4,\ R_5(2^3) = 3,\ R_5(2^4) = 1$

Anwendung

Wichtiges Instrument: Kleiner Satz von Fermat

$$R_p(a^p) = a \Longleftrightarrow R_p(a^{p-1}) = 1$$

$$(p \text{ Primzahl}, \ 0 < a < p)$$

$R_p(b) =$ Rest von b nach Division durch p

- $R_5(2^1) = 2, \ R_5(2^2) = 4, \ R_5(2^3) = 3, \ R_5(2^4) = 1$
- $R_5(3^1) = 3, \ R_5(3^2) = 4, \ R_5(3^3) = 2, \ R_5(3^4) = 1$

Anwendung

Wichtiges Instrument: Kleiner Satz von Fermat

$$R_p(a^p) = a \Longleftrightarrow R_p(a^{p-1}) = 1$$

$$(p \text{ Primzahl}, \ 0 < a < p)$$

$R_p(b) =$ Rest von b nach Division durch p

- $R_5(2^1) = 2, \ R_5(2^2) = 4, \ R_5(2^3) = 3, \ R_5(2^4) = 1$
- $R_5(3^1) = 3, \ R_5(3^2) = 4, \ R_5(3^3) = 2, \ R_5(3^4) = 1$
- $R_5(4^1) = 4, \ R_5(4^2) = 1, \ R_5(4^3) = 4, \ R_5(4^4) = 1$

Anwendung

- Public Key Kryptographie:

$$R_{p\cdot q}(a^{(p-1)(q-1)}) = 1$$

$$(p, q \text{ verschiedene Primzahlen})$$

- Sicherheit der Verschlüsselung:
  Schwierigkeit der schnellen Faktorisierung von $m = p \cdot q$ in die Primfaktoren p und q

Zählen von Primzahlen

Primzahlfunktion $\pi(x)$

- x positive, reelle Zahl
- $\pi(x) =$ Anzahl aller Primzahlen kleiner oder gleich x

$$= \sharp\{p = \text{Primzahl} \mid p \leq x\}$$

Primzahlfunktion $\pi(x)$

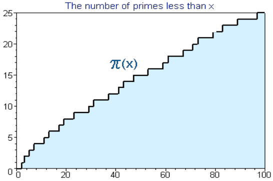
- x positive, reelle Zahl
- $\pi(x) =$ Anzahl aller Primzahlen kleiner oder gleich x

  $= \sharp\{p = \text{Primzahl} \mid p \leq x\}$
- $\pi(10) = 4$, $\pi(100) = 25$, $\pi(1000) = 168$

Primzahlfunktion $\pi(x)$

- x positive, reelle Zahl
- $\pi(x) =$ Anzahl aller Primzahlen kleiner oder gleich x

  $= \sharp\{p = \text{Primzahl} \mid p \leq x\}$
- $\pi(10) = 4,\ \pi(100) = 25,\ \pi(1000) = 168$

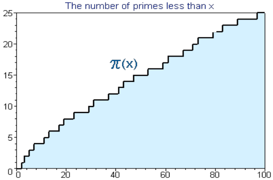


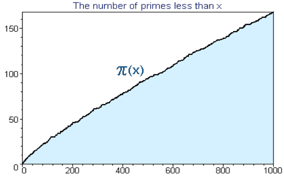
Primzahlfunktion $\pi(x)$

- x positive, reelle Zahl
- $\pi(x) =$ Anzahl aller Primzahlen kleiner oder gleich x

$$= \sharp\{p = \text{Primzahl} \mid p \leq x\}$$

- $\pi(10) = 4,\ \pi(100) = 25,\ \pi(1000) = 168$





Primzahlsatz

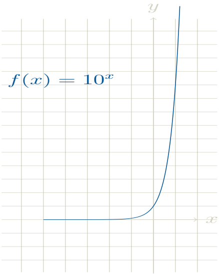
- Für $x \gg 0$, d.h. x sehr groß, gilt:

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

Primzahlsatz

- Für $x \gg 0$, d.h. x sehr groß, gilt:

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

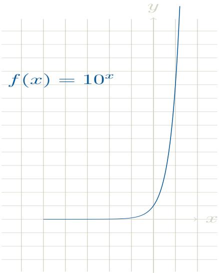


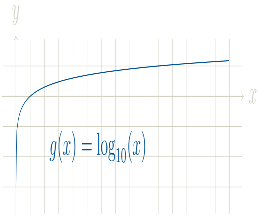
Primzahlen und Chaos
Jürg Kramer
Natürliche Zahlen
Bausteine
Primzahlen
Zählen von Primzahlen
Riemannsche Vermutung
Riemannsche Zetafunktion
Klassische Mechanik
Quantenmechanik

Primzahlsatz

- Für $x \gg 0$, d.h. x sehr groß, gilt:

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





Wie sind die Primzahlen verteilt?

- Also: Für $x \gg 0$ gilt:

$$\pi(x) \sim \frac{x}{\log(x)} \sim x^{1-\epsilon} \qquad (0 < \epsilon \ll 1).$$

- M.a.W. die Funktion $\pi(x)$ schmiegt sich für $x \to \infty$ immer mehr an die Funktion $x/\log(x)$ an.

- D.h. die Funktion

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

wächst für $x \to \infty$ von niedriger Ordnung als $x/\log(x)$.

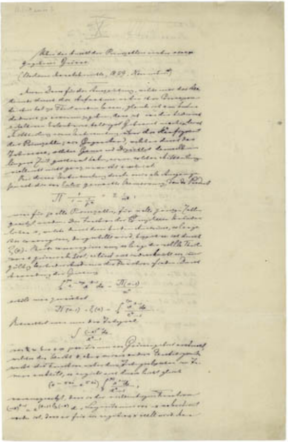
Milleniumsproblem

Die Riemannsche Vermutung:

Es existiert eine Konstante $C > 0$, so dass die Ungleichung

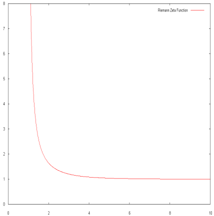
$$\left| \pi(x) - \frac{x}{\log(x)} \right| < C \cdot \sqrt{x}$$

für $x \to \infty$ besteht.



Riemannsche Zetafunktion

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$



- definiert schöne Funktion für $s > 1$,
- hat Pol erster Ordnung für $s = 1$.

Eulersche Produktentwicklung

Es besteht die Produktentwicklung

$$\zeta(s) = \prod_{p \text{ Primzahl}} \left(1 - \frac{1}{p^s}\right)^{-1}$$
$$= \frac{1}{1-2^{-s}} \cdot \frac{1}{1-3^{-s}} \cdot \frac{1}{1-5^{-s}} \cdot \frac{1}{1-7^{-s}} \cdots$$

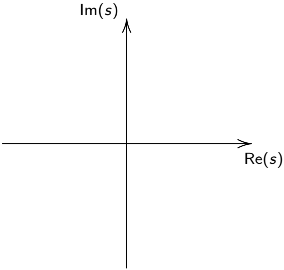
- Eulersche Produktentwicklung ist äquivalent zum Fundamentalsatz der Arithmetik.
- Der Pol erster Ordnung für $s = 1$ ist äquivalent zur Unendlichkeit der Primzahlmenge.

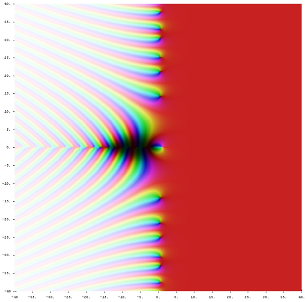
Komplexwertigkeit

Man kann $\zeta(s)$ auch als komplexwertige Funktion der komplexen Variablen

$$s = (\mathrm{Re}(s), \mathrm{Im}(s)) \Longleftrightarrow s = \mathrm{Re}(s) + i\,\mathrm{Im}(s)$$

auffassen. Sowohl Definitions- als auch Wertebereich sind dann reell 2-dimensional.

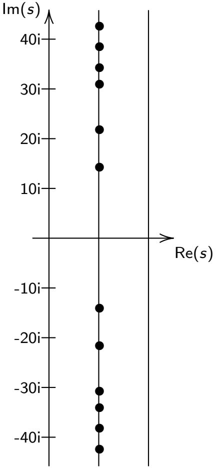




Äquivalente Umformulierung

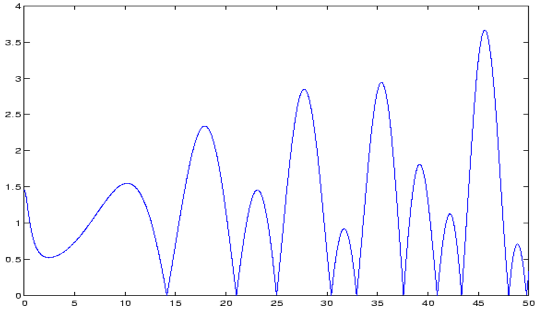
Äquivalente Umformulierung der Riemannschen Vermutung:

$\zeta(s)$ besitzt alle ihre (komplexen) Nullstellen bei $s = (1/2, \mathrm{Im}(s))$
(mit Ausnahme der „trivialen“ Nullstellen bei $s = -2, -4, -6, \ldots$).



Graph

Graph des Betrags der Riemannschen Zetafunktion auf der „kritischen Geraden" $\mathrm{Re}(s) = 1/2$, d.h. der Funktion $|\zeta(1/2 + it)|$ für $0 \leq t \leq 50$:



Klassische Mechanik

Bewegungsgleichung

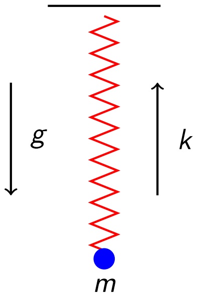
- Bei Angabe der Ausgangslage und der Anfangsgeschwindigkeit sowie der einwirkenden Kräfte kann die Bahnkurve eines Körpers (Lage, Geschwindigkeit) vorausbestimmt werden.

- Beispiel: Feder

$$m \cdot \ddot{x} = -k \cdot x$$

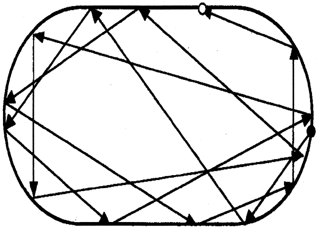
$$\Updownarrow \quad \lambda = -k/m$$

$$\frac{d^2}{dt^2} x(t) = \lambda \cdot x(t)$$



Klassisches Chaos

- Kleine Änderungen des Anfangszustands bewirken unvorhersehbare Änderungen des Endzustandes !
- Beispiel: Billardspiel
  Nach der 9. Banden-Berührung ist die Endrichtung der Billard-Kugel nicht mehr vorherbestimmbar !



Quantenmechanik

Problem: Es muss zwischen Observablen (Geschwindigkeit, ...) und Messwerten unterschieden werden. Messvorgang beeinflusst das Experiment!

Konsequenz:

Quantenmechanik

Problem: Es muss zwischen Observablen (Geschwindigkeit, ...) und Messwerten unterschieden werden. Messvorgang beeinflusst das Experiment!

Konsequenz:

- Physikalische Zustände entsprechen Vektoren Ψ in einem unendlich dimensionalen Vektorraum H.

Quantenmechanik

Problem: Es muss zwischen Observablen (Geschwindigkeit, ...) und Messwerten unterschieden werden. Messvorgang beeinflusst das Experiment!

Konsequenz:

- Physikalische Zustände entsprechen Vektoren Ψ in einem unendlich dimensionalen Vektorraum H.
- Beschreibung der Observablen durch lineare (selbstadjungierte) Operatoren A in H.

Quantenmechanik

Problem: Es muss zwischen Observablen (Geschwindigkeit, ...) und Messwerten unterschieden werden. Messvorgang beeinflusst das Experiment!

Konsequenz:

- Physikalische Zustände entsprechen Vektoren Ψ in einem unendlich dimensionalen Vektorraum H.
- Beschreibung der Observablen durch lineare (selbstadjungierte) Operatoren A in H.
- Die physikalischen Messwerte entsprechen den (reellen) Eigenwerten λ des Operators A.

Quantenmechanik

Problem: Es muss zwischen Observablen (Geschwindigkeit, ...) und Messwerten unterschieden werden. Messvorgang beeinflusst das Experiment!

Konsequenz:

- Physikalische Zustände entsprechen Vektoren Ψ in einem unendlich dimensionalen Vektorraum H.
- Beschreibung der Observablen durch lineare (selbstadjungierte) Operatoren A in H.
- Die physikalischen Messwerte entsprechen den (reellen) Eigenwerten λ des Operators A.
- Bewegungsgleichung gegeben durch die Schrödingergleichung

$$\frac{ih}{2\pi} \cdot \frac{\partial \Psi}{\partial t} = A \cdot \Psi,$$

wobei $h/2\pi = 1,054 \cdot 10^{-27} \mathrm{erg} \cdot \mathrm{s}$.

Quantenchaos

- Betrachte ein Billard-Spiel im Nanobereich ($\sim 10^{-9}\mathrm{m}$)
- Die Messwerte des quantenmechanischen Billard-Spiels sind gegeben durch die Eigenwertgleichung

$$A \cdot \Psi = \lambda \cdot \Psi$$

Quantenchaos

- Betrachte ein Billard-Spiel im Nanobereich ($\sim 10^{-9}\mathrm{m}$)
- Die Messwerte des quantenmechanischen Billard-Spiels sind gegeben durch die Eigenwertgleichung

$$A \cdot \Psi = \lambda \cdot \Psi$$

- Vermutung:
  Die Eigenwerte λ entsprechen den Nullstellen der Riemannschen Zetafunktion $\zeta(s)$ auf der kritischen Geraden $\mathrm{Re}(s) = 1/2$.