Freitag, 20. Nov. 2026: Beweis der

Riemannschen Vermutung

durch Levent Alpöge (Anthropic) mit Claude

- 17.000.000 Zeilen Lean-Code
- 250.000 Seiten Zusammenfassung

Riemannsche ζ-Funktion

$$\zeta(s) = \sum_{n \in \mathbb{N}} \frac{1}{n^s} = \prod_{p \text{ Primzahl}} \frac{1}{1 - p^{-s}}$$

$$\sum_{n \in \mathbb{N}} \frac{1}{n^s} \qquad \prod_{p \text{ Primzahl}} \frac{1}{1-p}$$

- Summe und Produkt konvergieren absolut für $s \in \mathbb{C}$ mit $\mathrm{Re}(s) > 1$
- Fortsetzung zu einer holomorphen Fkt. auf $\mathbb{C} \setminus \{1\}$ (bei $s=1$ Pol 1. Ordnung)
- triviale Nullstellen: $s = -2, -4, -6, \ldots$
  nichttriviale Nullstellen im Bereich $\{s \in \mathbb{C} \mid 0 < \mathrm{Re}(s) < 1\}$
- Riemannsche Vermutung (1859): Alle nichttrivialen haben Realteil $\frac{1}{2}$.
- Verbindung zu den Primzahlen
  primzahlzählende Fkt. $\pi(x) = |\{p \mid p \text{ Primzahl}, p \leq x\}|$

wird gut approximiert durch den

Integral logarithmus $\mathrm{Li}(x) = \int_2^x \frac{dt}{\ln(t)}$

bekannt: $\lim_{x \to \infty} \frac{\pi(x) - \mathrm{Li}(x)}{\mathrm{Li}(x)} = 0$

Man kann zeigen: Gilt $\mathrm{Re}(s) \leq \alpha$ für alle nicht-trivialen Nullstellen s von ζ (wobei $\frac{1}{2} \leq \alpha < 1$)

dann existiert eine Konstante $C \in \mathbb{R}^+$ mit

$|\pi(x) - \mathrm{Li}(x)| \leq C x^\alpha \ln(x)$ für x hinr. groß

(Für $\alpha < \frac{1}{2}$ ist das falsch.)

dann existiert eine Konstante $C \in \mathbb{R}^+$ mit

$$|\pi(x) - Li(x)| \leq C x^{\alpha} \ln(x) \quad \text{für } x \text{ hinr. groß}$$

- Analogon der Riemannschen ζ-Funktion für Kurven über endl. Körpern

q Primzahlpotenz > 1. $\mathbb{F}_q$ = Körper mit q Elementen

ebene Kurve über $\mathbb{F}_q$ = Nullstellenmenge eines Polynoms aus $\mathbb{F}_q[x,y]$ (z.zgl von Punkten im Unendlichen)

Zetafunktion der Kurve $C/\mathbb{F}_q$ = Potenzreihe $Z(C,t)$ in $\mathbb{Q}[[t]]$ mit $\frac{d}{dt} \ln Z(C,t) = \sum_{n=1}^{\infty} |C(\mathbb{F}_{q^n})| \, t^{n-1}$

Setze dann $\zeta_C(s) = Z(C, q^{-s})$

Gültigkeit der Riemannschen Vermutung für $\zeta_C(s)$ bekannt seit ca. 1940 (André Weil)

Definition der Kommutatorgruppe

Definition (6.6)

Sei G eine Gruppe. Für beliebige $g, h \in G$ bezeichnet man das Element $[g, h] = ghg^{-1}h^{-1}$ als den Kommutator von g und h. Bezeichnet $S = \{[g, h] \mid g, h \in G\}$ die Menge aller Kommutoren in G, so wird die Untergruppe $G' = \langle S \rangle$ die Kommutatorgruppe von G genannt.

Für alle $g, h \in G$ gilt jeweils

$$gh \quad = \quad [g, h]hg.$$

Die Bedeutung der Kommutatorgruppe

,

Satz (6.7)

Sei G eine Gruppe.

(i) Die Kommutatorgruppe G' ist ein Normalteiler von G.

(ii) Für einen beliebigen Normalteiler N von G gilt $N \supseteq G'$ genau dann, wenn die Faktorgruppe G/N abelsch ist.

Also ist G/G' die größte abelsche Faktorgruppe von G.

Beweis von Satz 6.7:

zu (i) $S = \{[g,h] \mid g,h \in G\}$, $G' = \langle S \rangle$

(wobei $[g,h] = ghg^{-1}h^{-1}$) zzg.: $G' \trianglelefteq G$

gleichbedeutend: $gG'g^{-1} \subseteq G' \quad \forall g \in G$

Sei also $g \in G$. Beh.: Es genügt zu überprüfen, dass $S \subseteq g^{-1}G'g$ gilt.

denn: $S \subseteq g^{-1}G'g$, $g^{-1}G'g \leq G$ (da $g^{-1}G'g$ Bild von $G' \leq G$ unter der Konjugation mit g^{-1} ist, und das ist ein Automorphismus)

$\Rightarrow \langle S \rangle \leq g^{-1} G' g \Rightarrow G' \leq g^{-1} G' g$

Daraus folgt $g G' g^{-1} \leq G'$. denn: Sei

$h \in g G' g^{-1} \Rightarrow \exists h_1 \in G' : h = g h_1 g^{-1}$

s.o. $\Rightarrow h_1 \in g^{-1} G' g$, d.h. $h_1 = g^{-1} h_2 g$ für ein

$h_2 \in G' \Rightarrow h = g h_1 g^{-1} = g (g^{-1} h_2 g) g^{-1}$

$= h_2 \in G'$ ($\Rightarrow$ Beh.)

Überprüfe nun $S \leq g^{-1} G' g$. Seien g_1, h_1

$\in G$, z.z.g.: $[g_1, h_1] \in g^{-1} G' g$. Es gilt

$$[g_1, h_1] = g_1 h_1 g_1^{-1} h_1^{-1} = g^{-1} g g_1 h_1 g_1^{-1} h_1^{-1} g^{-1} g$$

$$= g^{-1} (g g_1 g^{-1})(g h_1 g^{-1})(g g_1^{-1} g^{-1})(g h_1^{-1} g^{-1}) g =$$

$$= g^{-1} (g g_1 g^{-1})(g h_1 g^{-1})(g g_1 g^{-1})^{-1} (g h_1 g^{-1})^{-1} g$$

$g^{-1}\underbrace{[ggg^{-1}, ghg^{-1}]}_{\in G'}g \in g^{-1}Gg$

zu (ii) Sei N ein Normalteiler von G.

z.zg.: G/N ist abelsch $\iff N \supseteq G'$

„$\Leftarrow$" Seien $g, h \in G$. z.zg. $(gN)\cdot(hN) = (hN)\cdot(gN)$

äquivalent: $(gN)\cdot(hN)\cdot(gN)^{-1}\cdot(hN)^{-1} = e_{G/N}$

$\rightsquigarrow ghg^{-1}h^{-1}N = N \iff [g,h]N = N$

$\rightsquigarrow [g,h] N$. Dass G/N abelsch ist, ist also äquivalent dazu, dass N alle Kommutatoren enthält. Die Aussage $S \subseteq N$ ist gleichbed. mit $G' = \langle S \rangle \subseteq N$.

„$\Rightarrow$" G/N abelsch $\Rightarrow \forall g, h \in G$:

$(gN)(hN) = (hN)(gN) \overset{s.o.}{\Rightarrow} [g,h] \in N$

$\forall g, h \in G \Rightarrow S \subseteq N \Rightarrow G' = \langle S \rangle \subseteq N.$ □

Höhere Kommutatorgruppen und Auflösbarkeit

Man definiert rekursiv

- $G^{(0)} = G$
- $G^{(n+1)} = (G^{(n)})'$ für $n \in \mathbb{N}_0$

Die Untergruppen $G^{(n)}$ mit $n \geq 2$ werden die höheren Kommutatorgruppen von G genannt. Es gilt jeweils $G^{(n+1)} \trianglelefteq G^{(n)}$, und die Faktorgruppe $G^{(n)}/G^{(n+1)}$ ist abelsch.

Definition (6.8)

Eine Gruppe G wird auflösbar genannt, wenn $G^{(n)} = \{e\}$ für ein $n \in \mathbb{N}_0$ gilt.

Jede abelsche Gruppe G ist auflösbar, wegen $G^{(1)} = \{e\}$.

Definition der Subnormalreihen

Definition (6.9)

Eine Subnormalreihe für eine Gruppe G ist eine Folge von Untergruppen der Form

$$G = N_0 \supseteq N_1 \supseteq ... \supseteq N_r = \{e\}$$

mit $r \in \mathbb{N}_0$, wobei für $0 \leq k < r$ jeweils $N_{k+1} \trianglelefteq N_k$ gilt. Die Faktorgruppen N_k/N_{k+1} bezeichnet man als Faktoren der Subnormalreihe. Sind alle Faktoren abelsch, dann spricht man von einer abelschen Subnormalreihe.

Proposition (6.10)

Jede endliche abelsche Gruppe besitzt eine Subnormalreihe mit zyklischen Faktoren von Primzahlordnung.

Beweis von Proposition 6.10:

z.zg. Jede endl. G besitzt eine Subnormalreihe $G = N_0 \supseteq \dots \supseteq N_r = \{e\}$, wobei N_k/N_{k+1} zyklisch von Primzahlordnung für $0 \leq k < r$ ist. Beweis durch vollst. Ind. über $|G|$.

Ind.-Anf. $|G| = 1$ $G = \{e\}$, nichts zu zeigen (setze $N_0 = G$)

Ind.-schritt Sei $n = |G| > 1$, setze die Aussage für abelsche Gruppen kleinerer Ordnung voraus. Hauptsatz über endl. abelsche Gruppen $\Rightarrow$ G ist direktes Produkt von zykl. Gruppen $C_1, \dots, C_r$.

d.h. $G \overset{(*)}{\cong} C_1 \times \dots \times C_r$ mit $r \in \mathbb{N}$, $|C_i| > 1$ für $1 \leq i \leq r$

d.h. $G \cong C_1 \times \dots \times C_r$ mit $r \in \mathbb{N}$, $|C_i| > 1$ für $1 \leq i \leq r$

Wir können annehmen, dass (*) mit „=" gültig ist (statt „$\cong$").
Sei $g \in C_r$ mit $C_r = \langle g \rangle$ und p ein Primteiler von $\operatorname{ord}(g) = |C_r|$.
Dann gilt $\operatorname{ord}(g^p) = \frac{1}{p} \operatorname{ord}(g) < |C_r|$.
Setze nun $N_0 = G$ und $N_1 = C_1 \times \dots \times C_{r-1} \times \langle g^p \rangle$.
Dann gilt offenbar $|N_1| = \frac{1}{p}|N_0| < p$. Ind.-Vor. angewendet auf N_1 liefert eine Kette von Untergr. $N_1 \supseteq N_2 \supseteq \dots \supseteq N_r = \{e\}$
$\Rightarrow$ erhalte damit eine Kette $G = N_0 \supseteq N_1 \supseteq N_2 \supseteq \dots \supseteq N_r = \{e\}$
Dabei gilt jeweils $N_{k+1} \trianglelefteq N_k$ für $0 \leq k < r$ (für $k > 0$ nach Ind.-Vor., für $k = 0$ da G abelsch), und N_k / N_{k+1} ist jeweils zyklisch von Primzahlordnung (wieder für $k > 0$ nach Ind.-V., für $k = 0$ wegen $\frac{|N_0|}{|N_1|} = p$).
Damit ist der Ind.-schritt abgeschlossen. □

Auflösbarkeit und Subnormalreihen

Satz (6.11)

Für eine endliche Gruppe G sind die folgenden Eigenschaften äquivalent.

(i) Die Gruppe G ist auflösbar.

(ii) Sie besitzt eine abelsche Subnormalreihe.

(iii) Sie hat eine Subnormalreihe mit zyklischen Faktoren von Primzahlordnung.

Dabei ist die Äquivalenz „(i) $\Leftrightarrow$ (ii)“ auch für unendliche Gruppen gültig.

Beweis von Satz 6.11

Zeige zunächst nur die Äquivalenz von (i) und (ii).

„(i) ⇒ (ii)" G auflösbar ⇒ $\exists n \in \mathbb{N}_0 : G^{(n)} = \{e\}$

Für $0 \leq k < n$ gilt $G^{(k+1)} \trianglelefteq G^{(k)}$ und $G^{(k)}/G^{(k+1)}$ ist abelsch

⇒ Die höheren Kommutatorgruppen $G^{(k)}$ mit $0 \leq k \leq n$ bilden eine abelsche Subnormalreihe

„(ii) ⇒ (i)" Vor.: Es gibt eine abelsche Subnormalreihe $G = N_0 \supseteq N_1 \supseteq \dots \supseteq N_r = \{e\}$ mit $r \in \mathbb{N}_0$ (d.h. $N_{k+1} \trianglelefteq N_k$ und N_k/N_{k+1} ist abelsch für $0 \leq k < r$). Zzg: $\exists n \in \mathbb{N}_0$

mit $G^{(n)} = \{e\}$. Beh.: Für $0 \leq k \leq r$ gilt $G^{(k)} \subseteq N_k$.

(Daraus folgt insb. $G^{(r)} \subseteq N_r = \{e\}$ und somit $G^{(r)} = \{e\}$.)

Zeige die Beh. durch vollst. Ind. über k.

Ind.-Anf. $k=0$: Hier ist die Aussage offensichtlich, da nach Definition $G^{(0)} = G = N_0$ gilt.

Ind.-schritt $k \mapsto k+1$: Sei $k \in \{0, 1, \ldots, r-1\}$, setze $G^{(k)} \subseteq N_k$ voraus. $N_{k+1} \trianglelefteq N_k$ und N_k / N_{k+1} ist abelsch. Satz 6.7

$\Rightarrow N_{k+1} \geq N_k' \geq (G^{(k)})' = G^{(k+1)}$

Ein weiteres Auflösbarkeitskriterium

Satz (6.12)

(i) Jede Untergruppe einer auflösbaren Gruppe ist auflösbar.

(ii) Sei G eine Gruppe und $N \trianglelefteq G$. Unter diesen Voraussetzungen ist G auflösbar genau dann, wenn N und G/N beide auflösbar sind.