4 Beweise für die Unendlichkeit von Primzahlen

SEMIAR ELEGANTE BEWEISE WS 16/17

LUKAS RASCHKE

Agenda

1. Einleitung
    1. Primzahlen allgemein
    2. Relevanz von Primzahlen
2. Satz des Euklid
3. Brief v. Christian Goldbach an Euler
4. Mersenne-Zahlen
5. Harry Fürstenberg
6. Fazit und Ausblick

Primzahlen allgemein

- Form: $\boldsymbol{2k+1}$, $k \in \mathbb{N}$ Ausnahme: Zahl 2
  - nur durch sich selber und 1 teilbar
  - Alle Primzahlen ungerade

Relevanz

- Hauptsatz der elementaren Zahlentheorie
  - Jede natürliche Zahl lässt sich als Produkt von Primzahlpotenzen schreiben
  - Die Darstellung ist bis auf die Reihenfolge der Primzahlen eindeutig.

    → Primfaktorzerlegung

- Bis heute *KEINE* effiziente Methode zur Primfaktorzerlegung gefunden

  → Kryptografie

Satz des Euklid

- Annahme: Es gibt eine Menge endlich viele Primzahlen $\{P_1, P_2, P_3, \dots, P_i\}$

  P_k = größte bekannte Primzahl

- beliebige Zahl $n = P_1 \cdot P_2 \cdot P_3 \cdot \dots \cdot P_k + 1$

- Primfaktor $P_i \epsilon \mathbb{N}$ mit $P_i \mid n \quad \wedge \quad P_i \mid (n-1)$

  $\rightarrow P_i \mid (P_1 \cdot P_2 \cdot P_3 \cdot \dots \cdot P_k) + 1 \quad \wedge \quad P_i \mid (P_1 \cdot P_2 \cdot P_3 \cdot \dots \cdot P_k) \quad \rightarrow \quad P_i \mid 1$

- die Menge kann niemals *alle* Primzahlen enthalten

Brief v. Christian Goldbach an Euler

- Fermat-Zahlen: $\boldsymbol{F_n = 2^{2^n} + 1}$ mit $n \epsilon \mathbb{N}$

$F_0 = 3$

$F_1 = 5$

$F_2 = 17$

$F_3 = 257$

$F_4 = 65537$

$F_5 = 641 * 6700417$

Brief v. Christian Goldbach an Euler

- Zwei Fermat-Zahlen sind immer teilerfremd
- Menge der Fermat-Zahlen ist aufgrund von $\mathbb{N}$ unendlich

→ Jede Fermat-Zahl „verbraucht“ Primfaktoren Bsp.

→ Es muss unendlich viele Primzahlen geben

Brief v. Christian Goldbach an Euler

- Sei m ein gemeinsamer Teiler F_k von F_n und (mit $k < n$)

$$\prod_{k=0}^{n-1} F_k = F_n - 2 \qquad (n \geq 1)$$

→ m muss auch 2 teilen

- m = 1 oder 2

$$\boldsymbol{F_n = 2^{2^n} + 1}$$

→ der gemeinsame Teiler zweier Fermat-Zahlen ist die 1

Brief v. Christian Goldbach an Euler

- Verankerung: $n = 1$

$$\prod_{k=0}^{n-1} F_k = Fn - 2 \quad \rightarrow \quad 2^{2^0} + 1 = (2^{2^1}+1) - 2 \quad \rightarrow \quad 3 = 5 - 2 \ \checkmark$$

- Induktion: $n \rightarrow (n+1)$

$$\prod_{k=0}^{n} F_k = (\prod_{k=0}^{n-1} F_k) * Fn = (F_n - 2) * Fn$$

$$= (2^{2^n}-1)(2^{2^n}+1) = 2^{2^{n+1}} - 1 = Fn_{+1-2}$$ q.e.d

Mersenne-Zahl

- Es gibt eine größte Primzahl
- Erstellung einer Mersenne-Zahl mithilfe der Primzahl
- zu zeigen: Jeder Primteiler ist größer als die größte Primzahl

Mersenne-Zahl

$$M_n = 2^n - 1$$
$$M_0 = 0$$
$$M_1 = 1$$
$$M_2 = 3$$
$$M_3 = 7$$

- Annahme: P = größte bekannte Primzahl
- Mersenne-Zahl $2^P - 1$
- Primteiler q

$\rightarrow 2^P \equiv 1 \ (mod \ q)$

Mersenne-Zahl

- multiplikative Gruppe $\mathbb{Z}_q \setminus \{0\}$ des Körpers $\mathbb{Z}_q$
- Ordnung des Elements $\mathrm{o}(2\ \epsilon\ \mathbb{Z}_q \setminus \{0\}) = P$ (da P Primzahl)
- Anzahl der Elemente $|\mathbb{Z}_q \setminus \{0\}| = \mathrm{q} - 1$

Satz von Lagrange

Sei G eine endliche Gruppe.

(1) Ist H eine Untergruppe von G, so gilt $|H| \mid |G|$.

(2) Insbesondere teilt die Ordnung eines Elementes x von G die Gruppenordnung. Also für $x \in G$ gilt $|x| \mid |G|$.

Bsp.: $G = \mathbb{Z}_8^* = \{[1]_8, [3]_8, [5]_8, [7]_8\}$ o(3) = 2

$H = \mathbb{Z}_6^* = \{[1]_6, [5]_6\}$

Mersenne-Zahl

- Jedes Element der Gruppe teilt die Gruppengröße (2).

  → $\mathrm{P} \mid q - 1$

  → $\mathrm{P} < q$

- Der Primteiler q der Mersenne-Zahl ist größer als P.

  → Es gibt immer eine größere Primzahl

Beweis nach Euler

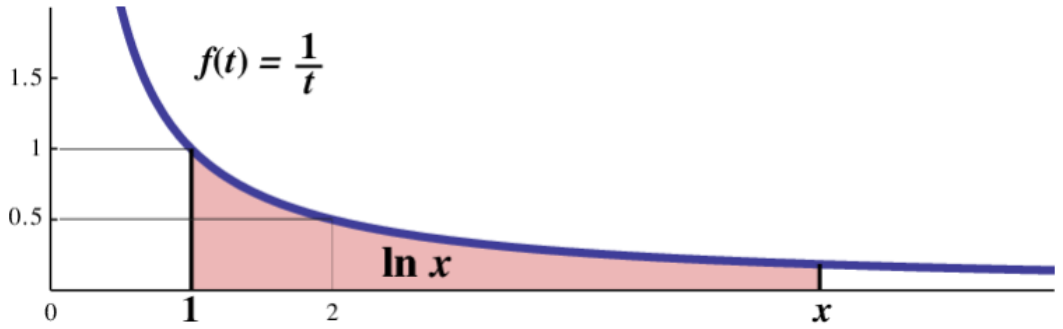
- Anzahl der Primzahlen kleiner einer reellen Zahl
- Vergleich zwischen der Fläche des natürlichen Logarithmus und einer oberen Treppenfunktion
- Ausnutzen der Tatsache, dass der Logarithmus unbeschränkt ist

Beweis nach Euler

- Sei $R(x) \coloneqq \#(p \leq x | p \in \mathbb{P}), x \in \mathbb{R}$

$$\mathbb{P} \coloneqq \{p_1, p_2, p_3, \dots\}$$

$$log(x) = \int_1^x \frac{1}{t} dt$$

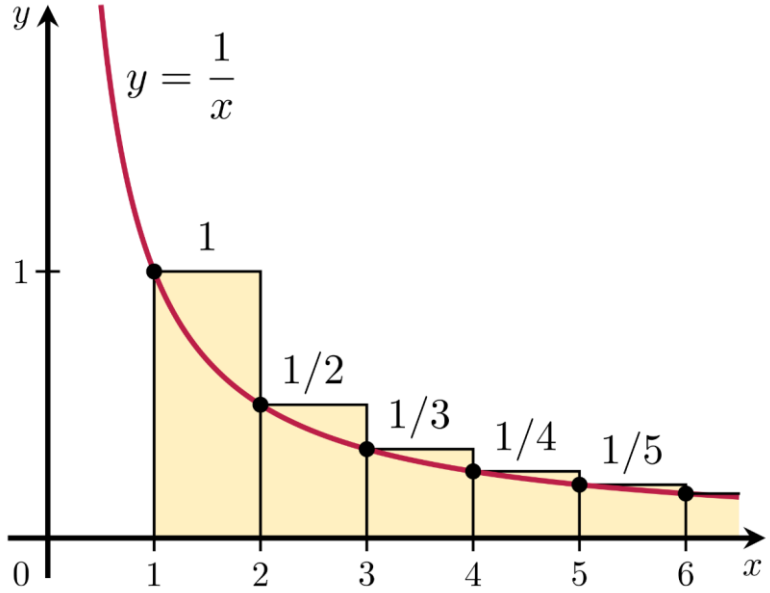


Beweis nach Euler

- für $n \leq x \leq n+1$:
- $log(x) \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1} + \frac{1}{n}$

$$\leq \sum{}' \frac{1}{m}$$

$m \in \mathbb{N}$, wobei m nur Primfaktoren $p \leq x$ enthält



Beweis nach Euler

- $log(x) \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1} + \frac{1}{n}$

$$\leq \sum{}' \frac{1}{m}$$

$$= \prod_{p \leq x} \left(\sum_{k \geq 0} \frac{1}{p^k} \right) \qquad \leq \prod_{p \leq x} \frac{1}{1 - \frac{1}{p}}$$

$$m = \prod_{p \leq x} p^k \qquad (p \in \mathbb{P})$$

Beweis nach Euler

$$\log(x) \leq \prod_{p \leq x} \frac{1}{1 - \frac{1}{p}}$$

$$= \prod_{p \leq x} \frac{p}{p-1} \qquad = \prod_{k=1}^{R(x)} \frac{p_k}{p_k - 1}$$

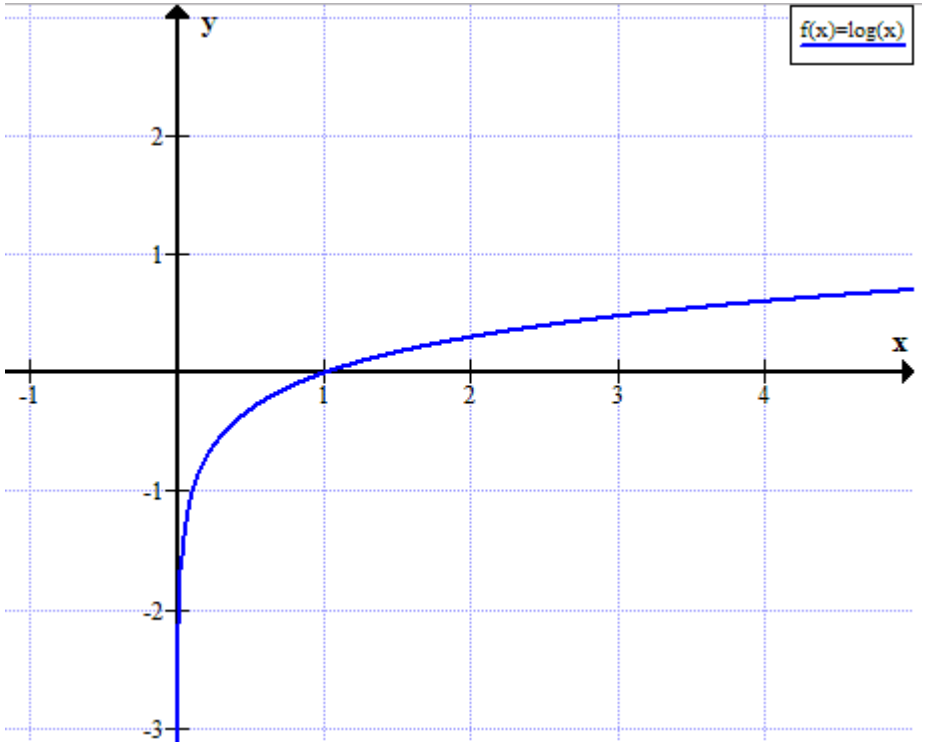
da $p_k \geq k + 1$

$$\frac{p_k}{p_k - 1} = 1 + \frac{1}{p_k - 1} \leq 1 + \frac{1}{k} = \frac{k+1}{k}$$

$$\leq \prod_{k=1}^{R(x)} \frac{k+1}{k} \qquad = R(x) + 1$$

$$\prod_{k=1}^{3} \frac{k+1}{k} = \frac{2}{1} * \frac{3}{2} * \frac{4}{3} = \frac{1}{1} * \frac{1}{1} * \frac{4}{1} = 4$$

Beweis nach Euler



$\log(x) \leq R(x) + 1$

$\log(x)$ ist unbeschränkt

→ $R(x) \coloneqq \#(p \leq x | p \in \mathbb{P}), x \in \mathbb{R}$ unbeschränkt

→ Es gibt unendlich viele Primzahlen

Fazit und Ausblick

- Diverse Ansätze, die Unendlichkeit der Primzahlen zu beweisen
  - Zahlentheorie
  - Analysis
  - Topologie
  - …