Die Unendlichkeit der Primzahlen

Vier Beweise von Euklid, Goldbach, Euler und Erdös

Was sind Primzahlen?

Definition

- Primzahlen sind natürliche Zahlen, die nur durch 1 und sich selbst teilbar sind
- 1 selbst ist keine Primzahl

Wissenschaftlich

- Die Menge der Primzahlen $\mathbb{P}$ ist wie folgt definiert:

$$\mathbb{P} := \{p \in \mathbb{N} : p \text{ ist prim}\}$$

Primfaktorzerlegung

- Ist Gegenstand des Fundamentalsatzes der Arithmetik

Definition

- Jede natürliche Zahl $n \in \mathbb{N}$ kann als Produkt aus Primzahlen $p \in \mathbb{P}$ dargestellt werden
- Dabei werden die p als Primfaktoren von n bezeichnet
- Insbesondere gilt die folgende Schreibweise mit $k \in \mathbb{N} \cup \{0\}$:

$$n := p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3} \cdot \ldots = \prod_{p \in \mathbb{P}} p^{k_p}$$

Beweis

- Sei $n \in \mathbb{N}$ eine beliebige Zahl

Fall 1

- n ist prim, dann kann es offensichtlich als Produkt von sich selbst geschrieben werden

Fall 2

- n ist nicht prim, dann kann n in zwei Faktoren aufgespalten werden
- Für beide Faktoren gilt erneut Fall 1 oder 2, demnach kann man sie so lange aufspalten, bis nur noch ein Produkt aus Primzahlen übrig bleiben

Beispiel

– Sei $n \coloneqq 90$

In welche Faktoren lässt sich n aufspalten?

Beispiel

- Sei $n := 90$
- $90 = 2 \cdot 45$ 2 ist prim | 45 ist nicht prim
- $45 = 3 \cdot 15$ 3 ist prim | 15 ist nicht prim
- $15 = 3 \cdot 5$ 3 ist prim | 5 ist prim

Also gilt:

$$90 = 2 \cdot 3 \cdot 3 \cdot 5$$

Besondere Schreibweise

- $90 = 2 \cdot 3 \cdot 3 \cdot 5 = 2^1 \cdot 3^2 \cdot 5^1 \cdot 7^0 \cdot 9^0 \dots$

$$p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3} \cdot \dots = \prod_{p \in \mathbb{P}} p^{k_p}$$

- Jede natürliche Zahl hat solch eine eindeutige Schreibweise
- Selbst die 1 kann wie folgt dargestellt werden:

$$1 = \prod_{p \in \mathbb{P}} p^0$$

Euklids Beweis

Teilerfremdheit

- Für jedes $a \in \mathbb{N}$ gilt, dass a und $a + 1$ teilerfremd sind, das heißt sie besitzen nur den gemeinsamen Teiler 1

Beweis

- Angenommen es gibt einen Teiler $b \in \mathbb{N}$ mit $b > 1$, dann existieren folgende Darstellungen:
- $a = kb$ und $a + 1 = lb$ mit $l, k \in \mathbb{N}$

Beweis

$$
\begin{aligned}
a + 1 &= lb \\
kb + 1 &= lb \\
1 &= lb - kb \\
1 &= b(l - k) \\
\frac{1}{b} &= l - k
\end{aligned}
$$

- Da l und k beide natürliche Zahlen sind, muss $\frac{1}{b}$ offensichtlich auch natürlich sein
- Dementsprechend muss $b = 1$ gelten

Euklids Beweis

Beweis per Widerspruch

- Sei $\mathbb{P} \coloneqq \{p_1, p_2, \ldots, p_k\}$ die endliche Menge der Primzahlen
- Sei $n \coloneqq p_1 \cdot p_2 \cdot \ldots \cdot p_k$ das Produkt aller Primzahlen
- Also ist $n + 1 = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$

Fall 1

- Angenommen $n + 1$ wäre prim, dann würde offensichtlich $n + 1 > p_k$ gelten, aber die größte Primzahl ist nach Definition p_k

$\Rightarrow$ Widerspruch

Euklids Beweis

Fall 2

- Also muss gelten, dass $n + 1$ nicht prim ist
- Demnach existiert eine Primfaktorzerlegung für $n + 1$
- Insbesondere existiert dann ein Primfaktor p für $n + 1$
- Da $n + 1$ und $n = p_1 \cdot p_2 \cdot ... \cdot p_k$ teilerfremd sind, muss p sich von jedem p_i unterscheiden
- Also liegt p nicht in der Menge der Primzahlen $\mathbb{P}$

$\Rightarrow$ Widerspruch

Euklids Beweis

- Wir haben erfolgreich gezeigt, dass $\mathbb{P}$ unendlich sein muss
- Ebenfalls stellt der Beweis einen Algorithmus dar, der immer eine neue Primzahl anhand einer endlichen Menge findet
- So kann man unendlich viele Primzahlen generieren

Algorithmus

```
[2, 3]
[2, 3, 7]
[2, 3, 7, 43]
[2, 3, 7, 43, 13]
[2, 3, 7, 43, 13, 53]
[2, 3, 7, 43, 13, 53, 5]
[2, 3, 7, 43, 13, 53, 5, 6221671]
[2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571]
[2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139]
[2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801]
[2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11]
[2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17]
[2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17, 5471]
```

Goldbachs Beweis

Mit Hilfe von Fermat-Zahlen

Fermat-Zahlen

Definition

$$F_n = 2^{2^n} + 1, \qquad n \in \mathbb{N}$$

Beispiele

$F_0 = 3$
$F_1 = 5$
$F_2 = 17$
$F_3 = 257$
$F_4 = 65537$
$F_5 = 4.294.967.297$

Rekursiver Hilfssatz

- Das Folgende soll für alle Fermat-Zahlen gelten:

$$\prod_{k=0}^{n-1} F_k = F_n - 2$$

- Diese Formel soll uns später helfen, zu zeigen, dass je zwei Fermat-Zahlen teilerfremd zueinander sind
- Aber erstmal kommen Beispiele und der Beweis

Beispiel

$$\prod_{k=0}^{n-1} F_k = F_n - 2$$

Rekursiver Anfang

$$\prod_{k=0}^{-1} F_k = 1 = F_0 - 2$$

$$F_0 = 3$$

Beispiel

- $F_0 = 3$
- Für $n = 1$ gilt:

$$\prod_{k=0}^{n-1} F_k = F_0 = F_1 - 2$$

$$F_1 = F_0 + 2$$

- Also ist $F_1 = 5$

Beispiel

- $F_0 = 3$
- $F_1 = 5$
- Für $n = 2$ gilt:

$$\prod_{k=0}^{n-1} F_k = F_0 \cdot F_1 = F_2 - 2$$

$$F_2 = F_0 \cdot F_1 + 2$$

Demnach ist F_2 was?

Beispiel

- $F_2 = F_0 \cdot F_1 + 2$
- $F_2 = 3 \cdot 5 + 2 = 17$

Induktiver Beweis

Induktionsanfang

– Bereits im Beispiel gezeigt

Induktionsannahme

$$\prod_{k=0}^{n-1} F_k = F_n - 2$$

Induktionsbehauptung

$$\prod_{k=0}^{n} F_k = F_{n+1} - 2$$

Induktiver Beweis

Induktionsschritt

$$\prod_{k=0}^{n} F_k = \left(\prod_{k=0}^{n-1} F_k\right) \cdot F_n \overset{IV}{=} (F_n - 2) \cdot F_n$$

$$\overset{Def.\,F_n}{=} \left(2^{2^n} + 1 - 2\right) \cdot \left(2^{2^n} + 1\right) = \left(2^{2^n} - 1\right) \cdot \left(2^{2^n} + 1\right)$$

$$\overset{Bin.\,Formel}{=} \left(2^{2^n}\right)^2 - 1 = 2^{2 \cdot 2^n} - 1 = 2^{2^{n+1}} - 1$$

$$= 2^{2^{n+1}} + 1 - 2 \overset{Def.\,F_n}{=} F_{n+1} - 2$$

Teilerfremdheit von Fermat-Zahlen

Behauptung

- Wir stellen folgende Behauptung auf:
- Für alle $n \in \mathbb{N}$ und $k \in \mathbb{N}$ mit $k < n$ gilt, dass $\mathrm{ggT}(F_k, F_n) = 1$

Beweis

- Sei $t \in \mathbb{N}$ ein Teiler von F_k und F_n, also gelte $t \mid F_k$ und $t \mid F_n$
- Dann gilt auch Folgendes:

$$t \mid F_n - F_k$$
$$t \mid F_n - F_0 \cdot \ldots \cdot F_k \cdot \ldots \cdot F_{n-1}$$

Teilerfremdheit von Fermat-Zahlen

- Aus dem Hilfssatz

$$\prod_{k=0}^{n-1} F_k = F_n - 2$$

- Und der Formel

$$t \mid F_n - F_0 \cdot \ldots \cdot F_k \cdot \ldots \cdot F_{n-1}$$

- Folgt dann:

$$t \mid F_n - (F_n - 2)$$
$$t \mid F_n - F_n + 2$$
$$t \mid 2$$

Teilerfremdheit von Fermat-Zahlen

- Aus $t \mid 2$ folgt demnach, dass $t = 1$ oder $t = 2$
- Aus der Definition von Fermat-Zahlen $F_n = 2^{2^n} + 1$ folgt jedoch:
$$2 \cdot 2^{2^n - 1} + 1 = 2 \cdot k + 1$$
- Da durch $2 \cdot k + 1$ jede Fermat-Zahl ungerade sein muss, kann nur $t = 1$ gelten

$\Rightarrow$ Der größte gemeinsame Teiler von je zwei Fermat-Zahlen ist 1

Goldbachs Beweis

- Mit $n \in \mathbb{N}$ existieren unendlich verschiedene Fermat-Zahlen $F_n = 2^{2^n} + 1$, die immer größer werden
- Durch die Primfaktorzerlegung existiert für jedes F_n ein Primfaktor p_n
- Dieser Primfaktor p_n kann kein Teiler von allen Fermat-Zahlen F_k mit $k < n$ sein, da sie teilerfremd zueinander sind
- Demnach existiert für jede Fermat-Zahl eine eindeutige Primzahl p_n

$\Rightarrow$ Die Menge $\{p_n : n \in N\} \subseteq \mathbb{P}$ ist unendlich

Eulers Beweis

Ein Beweis der Analysis

Motivation

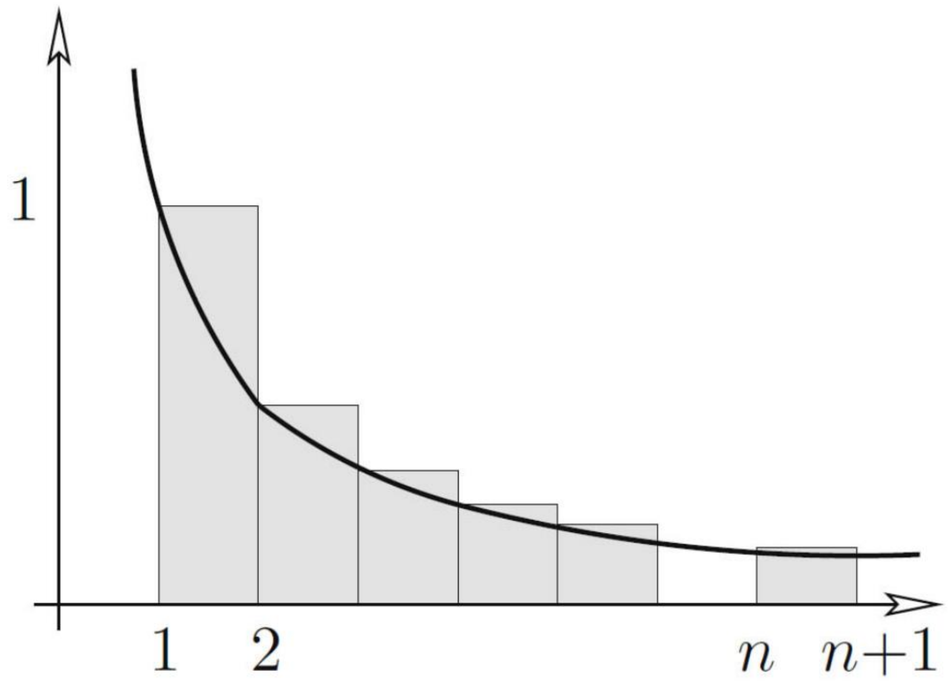
- Es wird die Funktion $\pi(x)$ definiert, die die Primzahlen kleiner als x zählt
- Der natürliche Logarithmus $\ln x$ wird nach oben mit $\pi(x) + 1$ abgeschätzt
- Also soll $\ln x \leq \pi(x) + 1$ gelten
- Da der Logarithmus unbeschränkt ist, folgt auch die Unbeschränktheit von $\pi(x)$

$\Rightarrow$ Die Anzahl der Primzahlen geht ins Unendliche

Logarithmische Funktion

- $\int_1^x \frac{1}{t}\,dt = \ln x - \underbrace{\ln 1}_{=0} = \ln x$
- Wir schätzen den Logarithmus mit der oberen Treppenfunktion ab
- Die graue Fläche umfasst dann für $n \leq x < n+1$:

$$1 \cdot \frac{1}{1} + 1 \cdot \frac{1}{2} + \cdots + 1 \cdot \frac{1}{n-1} + 1 \cdot \frac{1}{n}$$



Eine obere Treppenfunktion für $f(t) = \frac{1}{t}$

Obere Treppenfunktion

$$1 \cdot \frac{1}{1} + 1 \cdot \frac{1}{2} + \cdots + 1 \cdot \frac{1}{n-1} + 1 \cdot \frac{1}{n}$$

– Damit erhalten wir mit $n \leq x < n + 1$ die Abschätzung:

$$\ln x \leq \sum_{t=1}^{n} \frac{1}{t}$$

$\ln x \leq \sum_{t=1}^{n} \frac{1}{t}$

x	$\ln x$	$\sum_{t=1}^{n} \frac{1}{t}$
1	0	1
2	0.69	1.5
3	1.10	1.83
4	1.39	2.08
$\vdots$	$\vdots$	$\vdots$
1000	6.91	7.49

Weitere Abschätzungen

- Sei $m \in \mathbb{N}$ eine Zahl, die nur Primfaktoren $p \leq x$ enthält
- m kann als Primfaktorzerlegung wie folgt dargestellt werden:

$$m = \prod_{p \leq x} p^{k_p}$$

- Es gibt immer unendliche viele m, selbst für $x = 2$ gilt, dass $m = 2^k$ mit $k \in \mathbb{N}$ ist

Weitere Abschätzungen

- Es gilt demnach:

$$\ln x \leq \sum_{t=1}^{n} \frac{1}{t} \leq \sum \frac{1}{m}$$

- Die Summe geht über alle möglichen m
- Die Abschätzung gilt vor allem, da m alle t umfasst und noch unendliche viele Brüche mehr

Weitere Abschätzungen

– Wegen $m = \prod_{p \leq x} p^{k_p}$ kann die Summe wie folgt dargestellt werden:

$$\sum \frac{1}{m} = \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \left(\sum_{k \geq 0} \frac{1}{p^k} \right)$$

– Warum dies gilt, sieht man bestens an einem Beispiel

Beispiel

– Wir rechnen die Formel für $x = 3$ aus, also $p = 2$ und $p = 3$:

$$\prod_{\substack{p \in \mathbb{P} \\ p \le x}} \left(\sum_{k \ge 0} \frac{1}{p^k} \right) = \sum \frac{1}{2^k} \cdot \sum \frac{1}{3^k}$$

$$= \left(\frac{1}{1} + \frac{1}{2} + \frac{1}{4} + \cdots \right) \cdot \left(\frac{1}{1} + \frac{1}{3} + \frac{1}{9} + \cdots \right)$$

Beispiel

$$\left(\frac{1}{1}+\frac{1}{2}+\frac{1}{4}+\cdots\right)\cdot\left(\frac{1}{1}+\frac{1}{3}+\frac{1}{9}+\cdots\right)$$

– Wenn man nun alle Summanden miteinander multipliziert erhält man jede Kombination von $p = 2$ und $p = 3$, ähnlich wie bei der Primfaktorzerlegung

$$\frac{1}{1}\cdot\frac{1}{1}+\frac{1}{1}\cdot\frac{1}{3}+\cdots+\frac{1}{2}\cdot\frac{1}{1}+\frac{1}{2}\cdot\frac{1}{3}+\cdots$$

$$=\frac{1}{1}+\frac{1}{3}+\cdots+\frac{1}{2}+\frac{1}{6}+\cdots$$

Beispiel

- Es finden die gleichen Kombinationen statt wie bei der Primfaktorzerlegung
- Da m genauso definiert worden ist, folgt daraus:

$$\left(\frac{1}{1}+\frac{1}{2}+\frac{1}{4}+\cdots\right)\cdot\left(\frac{1}{1}+\frac{1}{3}+\frac{1}{9}+\cdots\right)=\sum\frac{1}{m}$$

- Also auch:

$$\sum\frac{1}{m}=\prod_{\substack{p\in\mathbb{P}\\ p\leq x}}\left(\sum_{k\geq 0}\frac{1}{p^k}\right)$$

Geometrische Reihe

– Für den nächsten Schritt brauchen wir die geometrische Reihe

Definition

– Für $q \in \mathbb{N}$ mit $|q| < 1$ gilt:

$$\sum_{k=0}^{\infty} q^k = \frac{1}{1-q}$$

Geometrische Reihe

- Offensichtlich gilt $\left|\frac{1}{p^k}\right| < 1$
- $\sum_{k\geq 0} \frac{1}{p^k}$ kann deshalb als geometrische Reihe erfasst werden und gleicht somit $\frac{1}{1-p}$
- Also kann man schreiben:

$$\sum \frac{1}{m} = \prod_{\substack{p\in\mathbb{P} \\ p\leq x}} \left(\sum_{k\geq 0} \frac{1}{p^k} \right) = \prod_{\substack{p\in\mathbb{P} \\ p\leq x}} \frac{1}{1-\frac{1}{p}}$$

Andere Schreibweise

$$\frac{1}{1-\frac{1}{p}} = \frac{1}{\frac{p}{p}-\frac{1}{p}} = \frac{1}{\frac{p-1}{p}} = \frac{p}{p-1}$$

– Mit Hilfe der Schreibweise folgt eine kleine Vereinfachung:

$$\sum \frac{1}{m} = \prod_{\substack{p\in\mathbb{P} \\ p\leq x}} \frac{1}{1-\frac{1}{p}} = \prod_{\substack{p\in\mathbb{P} \\ p\leq x}} \frac{p}{p-1}$$

Hauptidee

- Wir haben einiges an Vorarbeit geleistet, um gleich den Beweis zu beenden
- Vorher müssen wir noch ein paar Bezeichnungen definieren:

Primzählerfunktion

- Die Funktion $\pi(x)$ zählt alle Primzahlen, die kleiner als x sind
- Sie ist wie folgt definiert:

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

- Dabei sind die Primzahlen in aufsteigender Reihenfolge definiert, also mit $\mathbb{P} \coloneqq \{p_1, p_2, p_3, \ldots\} = \{2, 3, 5, \ldots\}$
- $\pi(5) = 3$ wäre ein Beispiel

Umformung

– Wir iterieren über alle Primzahlen $p \leq x$, durch die geordnete Schreibweise und der Zählerfunktion gilt deshalb:

$$\ln x \leq \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}$$

Zur Erinnerung

– Wir haben bisher Folgendes gezeigt:

1. Der natürliche Logarithmus kann durch die obere Treppenfunktion abgeschätzt werden:

$$\ln x \leq \sum_{t=1}^{n} \frac{1}{t}$$

Zur Erinnerung

– Wir haben bisher Folgendes gezeigt:

2. Die Summe über allen m, die nur aus Primzahlen $p \leq x$ bestehen, ist größer:

$$\ln x \leq \sum_{t=1}^{n} \frac{1}{t} \leq \sum \frac{1}{m}$$

Zur Erinnerung

– Wir haben bisher Folgendes gezeigt:

3. Die Summe konnte in ein Produkt umgeformt werden:

$$\ln x \leq \sum_{t=1}^{n} \frac{1}{t} \leq \sum \frac{1}{m} = \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \left(\sum_{k \geq 0} \frac{1}{p^k} \right)$$

Zur Erinnerung

– Wir haben bisher Folgendes gezeigt:

4. Das Produkt konnte mit Hilfe der Summe der geometrischen Reihe vereinfach werden:

$$\ln x \leq \sum_{t=1}^{n} \frac{1}{t} \leq \sum \frac{1}{m} = \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \left(\sum_{k \geq 0} \frac{1}{p^k} \right) = \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{p}{p-1}$$

Zur Erinnerung

– Wir haben bisher Folgendes gezeigt:

5. Mit Hilfe der Zählerfunktion wissen wir nun:

$$\ln x \leq \sum_{t=1}^{n} \frac{1}{t} \leq \sum \frac{1}{m} = \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \left(\sum_{k \geq 0} \frac{1}{p^k} \right) = \prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}$$

Ein paar letzte Umformungen

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

- Offensichtlich gilt $p_k \geq k + 1$, da die Primzahlen deutlich schneller wachsen als sie gezählt werden
- $p_1 = 2$ und $k + 1 = 2$
- $p_2 = 3$ und $k + 1 = 3$
- $p_3 = 5$ und $k + 1 = 4$

Ein paar letzte Umformungen

– Aus $p_k \geq k + 1$ folgt dann:

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

– Daraus erhalten wir:

$$\ln x \leq \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1} \leq \prod_{k=1}^{\pi(x)} \frac{k + 1}{k}$$

Letzter Schritt

– Die folgende Gleichung gilt:

$$\prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x) + 1$$

– Final erhalten wir:

$$\ln x \leq \pi(x) + 1$$

Kurzer Induktiver Beweis

Induktionsanfang

– $\pi(x) = 1$

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

Induktionsschritt

– $\pi(x) \rightarrow \pi(x) + 1$

$$\prod_{k=1}^{\pi(x)+1} \frac{k+1}{k} = \prod_{k=1}^{\pi(x)} \frac{k+1}{k} \cdot \frac{\pi(x)+1+1}{\pi(x)+1} = (\pi(x)+1) \cdot \frac{\pi(x)+2}{\pi(x)+1} = \pi(x) + 2$$

Bedeutung

$$\ln x \leq \pi(x) + 1$$

– Der Logarithmus ist unbeschränkt, das heißt, jede natürliche Zahl kann auf einen Wert der Funktion abgebildet werden

– Daraus folgt, dass die Primzählerfunktion $\pi(x)$ auch unbeschränkt ist

$\Rightarrow$ Es gibt unendlich viele Primzahlen

Beweis von Erdös

Idee des Beweises

- Wir zeigen, dass die Reihe $\sum_{p\in\mathbb{P}}\frac{1}{p}$ divergiert
- Angenommen es gibt endlich viele Primzahlen, dann würde die Reihe offensichtlich konvergieren
- Daraus können wir schließen, dass es unendlich viele Primzahlen geben muss, falls die Reihe divergiert

$$\sum_{p\in\mathbb{P}}\frac{1}{p}\to\infty\Rightarrow\#\mathbb{P}=\infty$$

Beweis per Widerspruch

- Als erstes nehmen wir an, dass $\sum_{p \in \mathbb{P}} \frac{1}{p}$ konvergiert
- Sei $(p_n)_{n \in \mathbb{N}}$ die Folge der Primzahlen in aufsteigender Ordnung
- Da es einen Grenzwert gibt, können wir die Reihe vorne so weit kürzen, dass für die Summe ab einem bestimmten k gilt:

$$\sum_{i \geq k+1} \frac{1}{p_i} < \frac{1}{2}$$

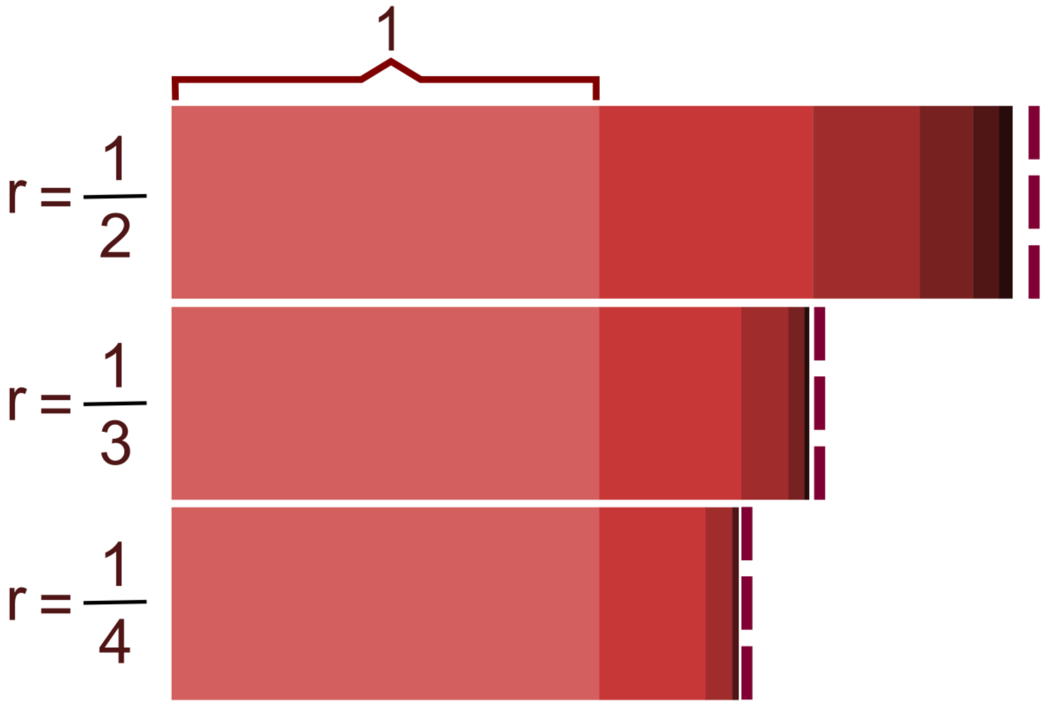
Beispiel an der Geometrischen Reihe

– Für $k = 1$ gilt die folgende Gleichung

$$\sum_{i \geq k+1} \frac{1}{2^k} < \frac{1}{2}$$

$$\frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \cdots < \frac{1}{2}$$

– Wir schneiden den Anfang ab



Modifikation

- Wir modifizieren die Summe, in dem wir die natürliche Zahl N dazu multiplizieren
- Für jedes beliebige $N \in \mathbb{N}$ gilt also:

$$\sum_{i \geq k+1} \frac{N}{p_i} < \frac{N}{2}$$

Definitionen

- Wir definieren für unser $k \in \mathbb{N}$ folgende Bezeichnungen:

Mengen

- $\mathcal{N}_s = \{p_1, \ldots, p_k\}$ sind kleine Primzahlen
- $\mathcal{N}_b = \{p_{k+1}, \ldots\}$ sind große Primzahlen

Anzahlen

- N_s ist die Anzahl der natürlichen Zahlen $n \leq N$, die nur durch kleine Primzahlen ($\in \mathcal{N}_s$) teilbar ist
- N_b ist die Anzahl der natürlichen Zahlen $n \leq N$, die mindestens durch eine große Primzahl ($\in \mathcal{N}_b$) teilbar ist

Beispiel

- Mit $k = 2$ und $N = 7$:

$$\sum_{i \geq 3} \frac{7}{p_i} < \frac{7}{2}$$

- $n \leq N$ bedeutet, dass $n \in \{1, 2, 3, 4, 5, 6, 7\}$
- $\mathcal{N}_s = \{2, 3\}$
- $\mathcal{N}_b = \{5, 7, 11, \dots\}$

Was sind N_s und N_b in diesem Fall?

Beispiel

- Die Zahl 1 ist hierbei ein Sonderfall, sie kann ausgeschlossen werden oder man zählt sie einfachheitshalber zu den kleinen Primzahlen
- $N_s = \#\{1, 2, 3, 4, 6\} = 5$
- $N_b = \#\{5, 7\} = 2$

Was fällt hier auf in Bezug auf $N = 7$?

Schlussfolgerung

- Es erschließt sich, dass $N_b + N_s = N$ ist
- Nach den Definitionen gilt dass für jedes N, da sich N_b und N_s gegenseitig ausschließen und den ganzen Bereich abdecken

Beweisidee

- Auf den nächsten Folien wollen wir den Widerspruch zeigen, dass auch $N_b + N_s < N$ gilt

Abschätzen von N_b

Definition

- N_b ist die Anzahl der natürlichen Zahlen $n \leq N$, die mindestens durch eine große Primzahl ($\in \mathcal{N}_b$) teilbar ist

Idee

- Wir beginnen damit, N_b abzuschätzen
- Dazu überlegen wir uns einen Weg, wie wir die Vorkommnisse, die zu N_b beitragen, zählen können

Abschätzen von N_b

Abschätzung

- Wir wollen also die Zahlen zählen, die mindestens eine große Primzahl $p \in \mathcal{N}_b$ enthalten
- Das heißt, wir wollen alle $n \leq N$ in der Form $n = p \cdot q$ haben, wobei $q \in \mathbb{N}$ ein beliebiger Faktor ist
- Wir können dies abschätzen, in dem wir für jedes p alle möglichen q zählen

Abschätzen von N_b

- Um die q zu zählen, verwenden wir Folgendes:

$$N_b \leq \left\lfloor \frac{N}{p_{k+1}} \right\rfloor + \left\lfloor \frac{N}{p_{k+2}} \right\rfloor + \cdots$$

- Es wird ab p_{k+1} gezählt, ab da fangen die großen Primzahlen nach Definition an
- Uns interessieren die $n \leq N$, deshalb nehmen wir die untere Schranke von N

Beispiel

- Mit $N = 10$ und $k = 1$:

$$N_b \leq \left\lfloor \frac{10}{3} \right\rfloor + \left\lfloor \frac{10}{5} \right\rfloor + \left\lfloor \frac{10}{7} \right\rfloor = 6$$

- Wir zählen damit:
- $\left\lfloor \frac{10}{3} \right\rfloor = 3 = \#\{3, 6, 9\}$
- $\left\lfloor \frac{10}{5} \right\rfloor = 2 = \#\{5, 10\}$
- $\left\lfloor \frac{10}{7} \right\rfloor = 1 = \#\{7\}$

Keine Gleichheit

$$N_b \leq \left\lfloor \frac{N}{p_{k+1}} \right\rfloor + \left\lfloor \frac{N}{p_{k+2}} \right\rfloor + \cdots$$

Weiß jemand, wieso $\leq$ gilt und nicht das Folgende?

$$N_b = \left\lfloor \frac{N}{p_{k+1}} \right\rfloor + \left\lfloor \frac{N}{p_{k+2}} \right\rfloor + \cdots$$

Keine Gleichheit

- Bei der Abschätzung können wir eventuell doppelte Vorkommnisse zählen, wenn eine Zahl aus zwei oder mehreren großen Primzahlen besteht
- Das spielt aber keine Rolle für die Effektivität des Beweises, da wir es sowieso nach oben abschätzen wollen

Abschätzen von N_b

– Mit unserer Vorarbeit können wir N_b weiter abschätzen:

$$N_b \leq \left\lfloor \frac{N}{p_{k+1}} \right\rfloor + \left\lfloor \frac{N}{p_{k+2}} \right\rfloor + \cdots \leq \sum_{i \geq k+1} \frac{N}{p_i} < \frac{N}{2}$$

– Also gilt:

$$N_b < \frac{N}{2}$$

Abschätzen von N_s

– Um N_s abzuschätzen, schreiben wir die $n \leq N$, die dazu zählen, als Primfaktorzerlegung auf:

$$n = \prod_{i=1}^{k} p_i^{m_i} = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_k^{m_k}$$

– Als nächstes wollen wir n in einen quadratfreien und nicht quadratfreien Teil aufteilen

Aufteilung

- Mit Hilfe der Primfaktorzerlegung können wir ziemlich einfach, den größten, quadratischen Teil aus n herausziehen
- Dazu ziehen wir von jedem $p_i^{m_i}$ den höchsten geraden Exponenten ab
- Diese Aufteilung bezeichnen wir mit $n = b_n^2 \cdot a_n$, wobei b_n^2 eine Quadratzahl und a_n ein quadratfreier Teil ist
- Das kann am besten mit einem Beispiel gezeigt werden:

Beispiel

- Sei $n = b_n^2 \cdot a_n = 2^5 \cdot 3^2 \cdot 5^0 \cdot 7^1 = 2016$

Quadratzahl

- Wir suchen uns von n die höchsten geraden Exponenten, dies ist unsere Quadratzahl $b_n^2 = 2^4 \cdot 3^2 \cdot 5^0 \cdot 7^0$
- Wir sehen, dass $b_n^2 = 144 = 12^2$ eine Quadratzahl ist

Quadratfreier Teil

- Der quadratfreie Teil a_n ist dann der Rest $a_n = 2^1 \cdot 3^0 \cdot 5^0 \cdot 7^1$
- Damit beträgt $a_n = 14$, insbesondere hat jede Primzahl in a_n nur den Exponenten 1 oder 0

Abschätzen von N_s

- Wir können n wie folgt beschreiben:

$$n = b_n^2 \cdot a_n = b_n^2 \cdot p_1^{\begin{bmatrix}1\\0\end{bmatrix}} \cdot p_2^{\begin{bmatrix}1\\0\end{bmatrix}} \cdot \ldots \cdot p_k^{\begin{bmatrix}1\\0\end{bmatrix}}$$

- Jedes $p_i^{\begin{bmatrix}1\\0\end{bmatrix}}$ hier kann entweder den Exponenten 1 oder 0 haben

Abschätzen von N_s

$$n = b_n^2 \cdot a_n = b_n^2 \cdot p_1^{\begin{bmatrix}1\\0\end{bmatrix}} \cdot p_2^{\begin{bmatrix}1\\0\end{bmatrix}} \cdot \ldots \cdot p_k^{\begin{bmatrix}1\\0\end{bmatrix}}$$

– Aus dieser Schreibweise wird klar, dass der quadratfreie Teil a_n genau 2^k Möglichkeiten hat, wie er zusammengesetzt werden kann

– Das liegt daran, dass man jede Wahl zwischen 1 und 0 k-mal wiederholt

Abschätzen von N_s

- Währenddessen gilt für die Quadratzahl Folgendes:

$$\begin{aligned} n &\leq N \\ b_n^2 &\leq n \\ b_n^2 &\leq N \\ b_n &\leq \sqrt{N} \end{aligned}$$

- Das heißt: b_n kann maximal $\lfloor \sqrt{N} \rfloor$-viele Werte annehmen
- Daraus lassen sich die Kombinationen für n berechnen

Abschätzen von N_s

- Wegen $n = b_n^2 \cdot a_n$ gibt es maximal $\sqrt{N} \cdot 2^k$ Kombinationen, wie n konstruiert werden kann
- Daraus folgt, dass $N_s \leq \sqrt{N} \cdot 2^k$

Wiederholung

- Wir haben bisher gezeigt, dass $N_b < \frac{N}{2}$ und dass $N_s \leq \sqrt{N} \cdot 2^k$
- Unser Ziel war es zu zeigen, dass es einen Widerspruch für $N_s + N_b = N$ gibt
- Für einen Widerspruch reicht es zu zeigen, dass ein bestimmtes N die Gleichung widerlegt

Widerspruch

– Sei $N = 2^{2k+2}$

$$N_b + N_s < \frac{N}{2} + \sqrt{N} \cdot 2^k$$

$$= \frac{2^{2k+2}}{2} + \sqrt{2^{2k+2}} \cdot 2^k = 2^{2k+1} + 2^{k+1} \cdot 2^k$$

$$= 2^{2k+1} + 2^{2k+1} = 2 \cdot 2^{2k+1} = 2^{2k+2}$$

– Aber 2^{2k+2} ist genau N
– Das heißt, wir haben gezeigt, dass $N_b + N_s < N$ gilt

Beweisende

- Unsere ursprüngliche Annahme war, dass $\sum_{p \in \mathbb{P}} \frac{1}{p}$ konvergiert
- Wenn das der Fall gewesen wäre, dann hätte nach unserer Definition $N_b + N_s = N$ für jedes N gelten müssen
- Das tut es aber nicht, wie wir es für $N = 2^{2k+2}$ mit der Gleichung $N_b + N_s < N$ gezeigt haben
- Also ist unsere Annahme, dass $\sum_{p \in \mathbb{P}} \frac{1}{p}$ konvergiert falsch

$\Rightarrow \sum_{p \in \mathbb{P}} \frac{1}{p}$ muss divergieren, daher gibt es auch unendliche viele Primzahlen

Ende der Präsentation

– Das waren vier Beweise zur Unendlichkeit der Primzahlen

Danke fürs Zuhören

Quellen

- Das BUCH der Beweise
- Detailliertere Erklärungen zu den Beweisen: https://www2.informatik.hu-berlin.de/~koessler/Proseminar/Proseminar2021/UnendlichVielePrimzahlenBirsul.pdf
- Euklids Beweis: https://www.youtube.com/watch?v=4QXzGE96Wpo
- Goldbachs Beweis: https://www.youtube.com/watch?v=pW2kaCJddYE
- Erdös Beweis: https://www.youtube.com/watch?v=KVLqy8w6qXg&t