Das Postulat von Bertrand

Marc-Jan Szpineter

Proseminar bei Prof. Kössler - Institut für Informatik - Humboldt Universität zu Berlin

8. Januar 2024

Vorweg: Es gibt beliebig große Lücken zwischen den Primzahlen

- Betrachte das Produkt N über alle Primzahlen $\leq k+1$:

$$N := \prod_{p \leq k+1, p\ prim} p$$

- Keine der k Zahlen $N+2, N+3, \ \ldots\ , N+k, N+(k+1)$ kann prim sein, denn:
- Jedes i mit $2 \leq i \leq k+1$ besitzt einen Primfaktor q mit $q \leq k+1$
- Der selbe Primfaktor q teilt natürlich auch N (enthält Produkt aller Primzahlen bis $\leq k+1$)
- $\implies q$ teilt auch $N+i$, mit $2 \leq i \leq k+1$

Das Theorem

Das Bertrandsche Postulat

Für jedes $n \geq 1$ ex. eine Primzahl p, s.d. gilt: $n < p \leq 2n$

Das Bertrandsche Postulat besagt damit, dass
"[...] die Lücke bis zur nächsten Primzahl nie größer sein kann als die Zahl, an der wir die Suche beginnen"

Geschichtliches

- Erstmals 1845 von Joseph Bertrand (1822-1900) vermutet
  - Bis $n = 3000000$ verifiziert
- Erster Beweis f.a. natürlichen $n \geq 1$: 1850 von Pafnuty Tschebyschew
- 1919: Einfacherer Beweis vom indischen Mathematiker Ramanujan
- 1932: ebenfalls einfacherer und elementarer Beweis von Paul Erdos (als er 19 war)
  - Seinen Beweis bzw. den Beweis aus dem BUCH (welches mit den Kernideen aus Erdos Beweis argumentiert) betrachten wir hier

Der BUCH-/Erdos Beweis

1. Beweis der Aussage bis $n < 512 = 2^9$ (mit "Landau-Trick")
2. z.Z.:
$$\prod_{p \leq x,\ p\ prim} p \leq 4^{x-1}$$
für alle $x \in \mathbb{R}$ mit $x \geq 2$
3. z.Z.: Sei p prim, $r \geq 1$ und es gelte $p^r \mid \binom{2n}{n} \implies p^r \leq 2n$
4. $\binom{2n}{n}$ nach unten abschätzen über $\frac{4^n}{2n} \leq \binom{2n}{n}$ und nach oben hin über die Primfaktorzerlegung von $\binom{2n}{n}$.
5. Anzahl $P(n)$ an Primzahlen zwischen n und $2n$ mit 0 annehmen und aus 4. daraus einen Widerspruch ableiten (Erdos).
Oder das Postulat aus 4. direkt beweisen (BUCH).

Schritt 1

z.Z.:

Für jedes $n \in N$ mit $1 \leq n < 512$ ex. eine Primzahl p, s.d. gilt: $n < p \leq 2n$

Schritt 1

- Für $n = 1$ gilt offensichtlich $1 < 2 \leq 2 \cdot 1$
- Sei $n \geq 2$. Wir beweisen nicht jeden Fall einzeln, sondern benutzen einen Trick vom Mathematiker Landau.
- Betrachte 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 521
- Ist eine aufsteigende Liste von Primzahlen
- Jede Zahl in der Liste (außer der 2) ist kleiner als 2 mal die vorhergehende Primzahl

$\implies$ Für jede Primzahl p_i in der Liste gilt: $p_i < p_{i+1} < 2p_i$

$\implies$ Für jede Zahl n mit $p_i < n < p_{i+1}$ gilt: $n < p_{i+1} < 2p_i < 2n$

Schritt 2

z.Z.:

$$\prod_{p \leq x,\ p\ prim} p \leq 4^{x-1}$$

für alle $x \in \mathbb{R}$ mit $x \geq 2$

Schritt 2

- Sei p im Folgenden immer prim
- Wir brauchen die Aussage nur für Primzahlen beweisen, denn:
- Sei q die größte Primzahl mit $q \leq x$.
- Wenn die Aussage für dieses q gilt, dann gilt offenbar

$$\prod_{p \leq x} p = \prod_{p \leq q} \leq 4^{q-1} \leq 4^{x-1}$$

- Beweis per vollständiger Induktion über die Anzahl der Primzahlen im Produkt

Schritt 2

I.A.:

Die erste Primzahl ist $q = 2$.

Es gilt

$$\prod_{p \leq q} p = 2 \leq 4 = 4^{2-1} = 4^{q-1}$$

Schritt 2

Sei nun q prim und $q > 2$.
Offensichtlich ist q ungerade und hat somit die Form $q = 2m + 1$

I.V.:

$$\prod_{p \leq x} p \leq 4^{x-1}$$

für alle $x \in \mathbb{R}$ mit $2 < x < q$

I.S.:

Es gilt

$$\prod_{p \leq 2m+1} p = \prod_{p \leq m+1} p \prod_{m+1 < p \leq 2m+1} p$$

$$\leq 4^m \binom{2m+1}{m} \leq 4^m 2^{2^m} = 4^m 4^m = 4^{2m} = 4^{q-1}$$

Denn: siehe nächste Folie

Schritt 2

1. $$\prod_{p \leq m+1} p \leq 4^m$$

   gilt nach I.V.

2. $$\prod_{m+1 < p \leq 2m+1} p \leq \binom{2m+1}{m}$$

   , denn
   $$\binom{2m+1}{m} = \frac{(2m+1)!}{(m)!(m+1)!}$$
   ist eine ganze Zahl und das Primzahl-Produkt links teilt davon den Zähler, nicht aber den Nenner!

Schritt 2

3.
$$\binom{2m+1}{m} \leq 2^{2m}$$

, denn die beiden Binomialkoeffizienten

$$\binom{2m+1}{m} = \binom{2m+1}{m+1}$$

sind in der Summe

$$\sum_{k=0}^{2m+1} \binom{2m+1}{k} = 2^{2m+1} = 2 \cdot 2^{m}$$

enthalten.

Schritt 3

z.Z.:

Sei p prim, $r \geq 1$ und es gelte $p^r \mid \binom{2n}{n}$

$$\implies p^r \leq 2n$$

Schritt 3

Der Satz von Legendre:

$n!$ enthält den Primfaktor p

$$\sum_{k \geq 1} \left(\left\lfloor \frac{n}{p^k} \right\rfloor \right)$$

mal.

Beweis: Betrachte $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$
p teilt $\left\lfloor \frac{n}{p^1} \right\rfloor$ der Faktoren von $n!$.
p^2 teilt zusätzlich $\left\lfloor \frac{n}{p^2} \right\rfloor$ der Faktoren von $n!$.
Usw., wobei die Summenglieder ab $p^k > n$ verschwinden.

Schritt 3

Wir betrachten

$$\binom{2n}{n} = \frac{(2n)!}{n!n!}$$

Nach dem Satz von Legendre enthält $\binom{2n}{n}$ den Primfaktor p genau

$$r := \sum_{k \geq 1} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right)$$

mal.
Dabei gilt:

$$\left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right) < \frac{2n}{p^k} - 2 \left(\frac{n}{p^k} - 1 \right) = 2$$

Schritt 3

- $\implies$ Jeder Summand ist ≤ 1, da ganzzahlig.
- Ab $p^k > 2n$ ist jeder Summand 0
- $\implies p^r \leq 2n$

Schritt 4

$\frac{4^n}{2n} \leq \binom{2n}{n}$:

- $\binom{2n}{n}$ ist der größte Term von allen Binomialkoeffizienten $\binom{2n}{k}$, $0 \leq k \leq 2n$
-

$$4^n = 2^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} = 1 + 1 + \sum_{k=1}^{2n-1} \binom{2n}{k} = 2 + \sum_{k=1}^{2n-1} \binom{2n}{k}$$

$$4^n \leq 2n \binom{2n}{n}$$

$$\implies \frac{4^n}{2n} \leq \binom{2n}{n}$$

Schritt 4

Um nun $\binom{2n}{n}$ nach oben abzuschätzen, betrachten wir dessen Primfaktoren p in 4 Bereichen:

1. $p < \sqrt{2n}$
2. $\sqrt{2n} < p \leq \frac{2}{3}n$
3. $\frac{2}{3}n < p \leq n$
4. $n < p \leq 2n$

- Alle Primzahlen p mit $p^k > \sqrt{2n}$ kommen höchstens einmal vor
- Laut Erdos am wichtigsten: Primzahlen p im 3. Bereich, kommen gar nicht vor!
  Denn: siehe nächste Folie

Schritt 4

- Sei p Primzahl mit $\frac{2}{3}n < p \leq n$ und $n \geq 3$ (d.h. $p \geq 3$).
- $\implies 2n < 3p$
- Betrachte $\binom{2n}{n} = \frac{(2n)!}{n!n!}$
- $\binom{2n}{n}$ ist durch p, mit $\frac{2}{3}n < p \leq n$ und $2p$, mit $\frac{4}{3}n < 2p \leq n$ im Zähler teilbar.
- Im Nenner ist $\binom{2n}{n}$ nur jeweils einmal, also insgesamt zweimal durch p teilbar.
- $\implies p$ kürzt sich vollständig raus.

Schritt 4

Zusammenfassend ergibt sich mit den bisherigen Überlegungen insgesamt für $n \geq 3$:

- $$\frac{4^n}{2n} \leq \binom{2n}{n} \leq \prod_{p \leq \sqrt{2n}} 2n \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \cdot \prod_{n < p \leq 2n} p$$
- Sei $P(n) :=$ Anzahl an Primzahlen zw. n und $2n$.
- Da für jede Primzahl p, mit $r \geq 1$, die $\binom{2n}{n}$ teilt, immer gilt $p^r \leq 2n$, folgt:
  siehe nächste Folie

Schritt 4

$$\frac{4^n}{2n} \leq \binom{2n}{n} < (2n)^{\sqrt{2n}} \cdot 4^{\frac{2}{3}n} \cdot (2n)^{P(n)}$$

$$\implies 4^{\frac{1}{3}n} < (2n)^{\sqrt{2n}+1+P(n)}$$

Schritt 5

- Wir stellen nun nach P(n) um
- Dazu nehmen wir den Logarithmus zur Basis 2 und formen nach P(n) um:

$$\log_2\left(4^{\frac{1}{3}n}\right) < \log_2\left((2n)^{\sqrt{2n}+1+P(n)}\right)$$

$$\Leftrightarrow \frac{1}{3}n \cdot \log_2(4) < (\sqrt{2n} + 1 + P(n)) \cdot \log_2(2n)$$

$$\Leftrightarrow \frac{2n}{3 \cdot \log_2(2n)} < \sqrt{2n} + 1 + P(n)$$

$$\Leftrightarrow \frac{2n}{3 \cdot \log_2(2n)} - (\sqrt{2n} + 1) < P(n)$$

Schritt 5

- Wenn wir jetzt zeigen, dass $P(n) > 0$ für hinreichend große n, dann ist der Beweis vollständig
- Dazu zeigen wir

$$\frac{2n}{3 \cdot \log_2(2n)} - (\sqrt{2n} + 1) > 0$$

f.a. $n \geq 2^9 = 512$, was äquivalent ist zu

$$\frac{2n}{3 \cdot \log_2(2n)} > (\sqrt{2n} + 1)$$

f.a. $n \geq 2^9 = 512$

- Das wiederum zeigen wir mit einer stärkeren Aussage, indem wir $2n - 1 < 2n$ für den Zähler wählen:
siehe nächste Folie

Schritt 5

- Wir beweisen

$$\frac{2n}{3 \cdot \log_2(2n)} > \frac{2n-1}{3 \cdot \log_2(2n)} > (\sqrt{2n}+1)$$

  f.a. $n \geq 2^9 = 512$
- Das erste $>$ ist klar, also zeigen wir das zweite $>$
- Schreiben wir $2n - 1 = (\sqrt{2n}+1)(\sqrt{2n}-1)$, dann erhalten wir:

$$\frac{(\sqrt{2n}+1)(\sqrt{2n}-1)}{3 \cdot \log_2(2n)} > (\sqrt{2n}+1)$$

$$\Leftrightarrow (\sqrt{2n}-1) > 3 \cdot \log_2(2n)$$

- Diese Ungleichung gilt für $n = 2^9 = 512$:
  $31 > 30$

Schritt 5

- Vergleichen wir die Ableitungen beider Funktionen miteinander, dann ergibt sich:

$$(\sqrt{x}-1)' = \frac{1}{2}\cdot\frac{1}{\sqrt{x}}$$

$$(3\cdot\log_2(2x))' = \frac{3}{\ln(2)}\cdot\frac{1}{x}$$

- Dabei wächst $(\sqrt{x}-1)'$ bereits schneller ab etwa $x > 75$
- Da wir in Schritt 1 bereits den Fall $n < 512$ gezeigt haben, ist das Postulat damit bewiesen. $\square$

Quellen

- "Das BUCH der Beweise", 5.Auflage, Martin Aigner, Günter M. Ziegler
- Wikipedia: Bertrand's postulate
- Wikipedia: Proof of Bertrand's postulate
- "Beweis eines Satzes von Tschebyschef.", P. Erdos, 1932