BERTRANDs Postulat

von NIKO WILBERT

Hintergrund

Wie wir in einem anderen Vortrag sehen werden ist die Anzahl der Primzahlen unendlich. Gleichzeitig ist jedoch der Abstand zweier Primzahlen nicht beschränkt.

> Beweis:
> Definiere die Zahl $N := 2 \cdot 3 \cdot \ldots \cdot p$ als das Produkt aller Primzahlen, die kleiner als $k+2$ sind ($k \in \mathbb{N}$). Es stellt sich nun heraus, dass von den k Zahlen
>
> $$N+2,\ N+3,\ \ldots,\ N+(k+1) \quad \text{bzw.} \quad N+i \quad \text{mit} \quad 2 \leq i \leq k+1,\ i \in \mathbb{N}$$
>
> keine einzige prim ist. Dies liegt daran, dass die Primfaktoren von i immer auch N teilen. Also läßt sich auch $N+i$ durch die Primfaktoren von i teilen und ist daher keine Primzahl.
> Auf diese Weise hat man also einen Bereich der Länge k gefunden, der keine Primzahl enthält.

Der Abstand von Primzahlen lässt sich aber auch nach oben eingrenzen. Besonders bekannt ist BERTRANDs Postulat, es lautet:

Für jedes $n \in \mathbb{N}$ existiert eine Primzahl p mit $n < p \leq 2n$.

Dieses soll nun gezeigt werden, wobei der Beweis 1932 von PAUL ERDŐS im Alter von 19 Jahren veröffentlicht wurde.

Der "Book Proof" von ERDŐS

Der Beweis erfolgt in 5 Schritten. Alle Buchstaben bezeichnen, sofern nicht anders angegeben, natürliche Zahlen. Bei p's soll es sich immer um Primzahlen handeln.
Dem Beweis liegt die Idee zugrunde $\binom{2n}{n}$ als Produkt von Primzahlen abzuschätzen, wobei die Annahme dass zwischen n und $2n$ keine Primzahlen existieren auf einen Widerspruch führt.

1. Schritt

Wir beweisen BERTRANDs Postulat für $n < 4000$. Dafür müssen jedoch nicht alle 3999 Fälle überprüft werden, sondern man wendet LANDAUs Trick an. Danach genügt es zu zeigen, dass die Zahlen

$$2,\ 3,\ 5,\ 7,\ 13,\ 23,\ 43,\ 83,\ 163,\ 317,\ 631,\ 1259,\ 2503,\ 4001$$

prim sind. Da jede kleiner als das Doppelte ihres Vorgängers ist liegt in jedem Intervall $(n;2n]$ mindestens eine von ihnen.

> *Beweis:* Sei $n < 4000$ beliebig und sei $i = \max\{j \,|\, p_j \leq n\}$ die nächstkleinere Primzahl aus der oben gegebenen Liste p_i. Die nächste Primzahl p_{j+1} ist dann kleiner als $2p_j \leq 2n$ und größer als n. p_{j+1} liegt also auf jeden Fall im Intervall $(n;2n]$.

2. Schritt

Als nächstes wird gezeigt, dass gilt

$$\prod_{p \leq x} p \;\leq\; 4^{x-1} \qquad \forall\, 2 \leq x \in \mathbb{R}$$

Sei q die größte Primzahl $\leq x$. Dann gilt natürlich $4^{q-1} \leq 4^{x-1}$ weshalb man o.B.d.A. annehmen darf, dass x eine Primzahl ist.
Da die Ungleichung für $x = 2$ außerdem erfüllt ist $(2 \leq 4)$ müssen nur noch ungerade Primzahlen berücksichtigt werden, also die Zahlen der Form $x = 2m + 1$. Der Beweis erfolgt nun durch Induktion nach m.
IA: Für $m = 1$ gilt die Ungleichung, denn $2 \cdot 3 = 6 \leq 16 = 4^{3-1}$.
IS: Es gilt

$$\prod_{p \leq 2m+1} p \;=\; \prod_{p \leq m+1} p \cdot \prod_{m+1 < p \leq 2m+1} p \qquad (*)$$

Nach Induktionsvoraussetzung[1] gilt für den ersten Faktor

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

Für den zweiten Faktor gilt die Ungleichung

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

> *Beweis*: Wie in Ana I gezeigt wurde ist $\binom{2m+1}{m} \in \mathbb{N}$, es gilt
>
> $$\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}$$
>
> Die Primzahlen p aus dem Produkt kommen bei diesem Bruch auf jeden Fall im Zähler vor, jedoch nicht im Nenner (da dieser aus Faktoren kleiner gleich $m+1$ besteht). Also teilt das Produkt der p den Binomialkoeffizienten, womit die Aussage bewiesen ist.

Als nächstes wird noch $\binom{2m+1}{m}$ nach oben abgeschätzt.

> Wie in Ana I gezeigt wurde gilt[2]
>
> $$\sum_{k=0}^{2m+1} \binom{2m+1}{k} = 2^{2m+1}$$
>
> Da $\binom{2m+1}{m}$ und $\binom{2m+1}{m+1}$ zwei gleiche Summanden dieser Summe sind folgt
>
> $$\binom{2m+1}{m} \;\leq\; 2^{2m}$$

Also läßt sich Ungleichung $(*)$ abschätzen zu

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

[1] Wobei man sich auch hier einfach auf die nächstkleinere Primzahl zurückziehen kann.
[2] Betrachte einfach $2^n = (1+1)^n$.

3. Schritt

Hier wird nun zunächst Legendres Theorem benötigt. Es lautet

Die Zahl $n!$ enthält den Primfaktor p genau $\sum_{k\geq 1}\left\lfloor \frac{n}{p^k}\right\rfloor$ mal.

Beweis: Von den Faktoren von $n!$ lassen sich genau $\left\lfloor \frac{n}{p}\right\rfloor$ durch p teilen, denn es gibt genau $\left\lfloor \frac{n}{p}\right\rfloor$ Vielfache von p die kleiner gleich n sind.
Analog lassen sich genau $\left\lfloor \frac{n}{p^2}\right\rfloor$ Faktoren von $n!$ durch p^2 teilen. Da diese auch schon bei der vorigen Zählung berücksichtigt wurden, reicht es aus, sie hier nur einfach zu berücksichtigen.
Der Beweis lässt sich nun in dieser Weise fortsetzen.

Wende dies nun auf $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ an indem man die Anzahl der Vorkommen im Nenner von denen im Zähler abzieht. Insgesamt kommt p also genau

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

mal als Primfaktor in $\binom{2n}{n}$ vor.
Zeige nun, dass die einzelnen Summanden nur den Wert 1 oder 0 haben.

Beweis: Der erste Teil lässt sich nach oben abschätzen durch

$$\left\lfloor \frac{2n}{p^k}\right\rfloor \leq \frac{2n}{p^k}$$

und der zweite nach unten mit

$$\left\lfloor \frac{n}{p^k}\right\rfloor > \frac{n}{p^k} - 1$$

Insgesamt also

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

Da der Ausdruck außerdem eine positive ganze Zahl ist folgt die Behauptung.

Für $p^k > 2n$ verschwindet der Summand sowieso, d.h. maximal haben $\max\{r \mid p^r \leq 2n\}$ Summanden den Wert 1.
Insbesondere ist eine Primzahl mit $p^2 > 2n \Leftrightarrow p > \sqrt{2n}$ höchstens ein einfacher Teiler von $\binom{2n}{n}$.

Eine Schlüsselrolle im Beweis hat nun die Feststellung, dass Primzahlen mit $\frac{2}{3}n < p \leq n$ für $n \geq 3$ (und somit auch $p \geq 3$) gar keine Teiler von $\binom{2n}{n}$ sind.

Beweis: Eine Primzahl mit $3p > 2n$ kommt nur zweimal im Zähler von $\frac{(2n)!}{n!n!}$ vor, nämlich als p und $2p$. Höhere Potenzen sind sowieso ausgeschlossen, da wegen $p \geq 3$ auch $p^2 \geq 3p > 2n$ ist. Insgesamt taucht also p in der Primfaktorzerlegung des Zählers mit dem Exponenten 2 auf.
Gleichzeitig kommt p jedoch auch genau einmal als Primfaktor in $n!$ vor, also taucht p auch in der Primfaktorzerlegung des Nenners mit dem Exponenten 2 auf.

4. Schritt

Nun soll endlich $\binom{2n}{n}$ abgeschätzt werden. Nach unten gilt

$$\binom{2n}{n} \geq \frac{4^n}{2n}$$

Beweis: Wie bereits bekannt gilt $\left[\binom{2n}{0} + \binom{2n}{2n}\right] + \sum_{i=1}^{2n-1} \binom{2n}{i} = 2^{2n} = 4^n$. Der größte (im Sinne von $\geq$) Summand dieser Summe ist immer $\binom{2n}{n}$.
Der arithmetische Mittelwert dieser Summe ist $\frac{4^n}{2n}$ und $\binom{2n}{n}$ ist als größter Summand mindestens so groß wie der Mittelwert.

Nach oben lässt sich $\binom{2n}{n}$ mit den Mitteln aus dem letzten Schritt und für $n \geq 3$ (siehe Schritt 3) als Produkt von Primzahlen abschätzen durch

$$\binom{2n}{n} \leq \prod_{p \leq \sqrt{2n}} 2n \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \cdot \prod_{n < p \leq 2n} p$$

mit den folgenden Begründungen:

- Wie im vorigen Schritt gezeigt geht ein Primfaktor höchstens mit der Potenz $\max\{r \mid p^r \leq 2n\}$ ein, sein Beitrag ist also immer kleiner gleich $2n$.
- Primfaktoren p mit $p > \sqrt{2n}$ kommen höchstens in einfacher Potenz vor.
- Primfaktoren p mit $\frac{2}{3}n < p \leq n$ kommen gar nicht vor.

Da es außerdem nicht mehr als $\sqrt{2n}$ Primzahlen mit $p \leq \sqrt{2n}$ geben kann gilt also insgesamt (nach Multiplikation mit $2n$)

$$4^n \leq (2n)^{1+\sqrt{2n}} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \cdot \prod_{n < p \leq 2n} p$$

5. Schritt

Angenommen es gäbe nun keine Primzahl p mit $n < p \leq 2n$, dann ist das letzte Produkt aus dem Ende des vorigen Abschnitts leer und hat somit den Wert 1.
Das mittlere Produkt wird nun mit der im zweiten Schritt des Beweises hergeleiteten Formel nach oben abgeschätzt. Dabei wird zum einen vernachlässigt, dass nur Primzahlen größer $\sqrt{2n}$ in dem Produkt stehen[3]. Zum anderen wird beim Ergebnis der Abschätzung $4^{\frac{2}{3}n-1}$ die -1 vernachlässigt.
Man erhält so die neue Ungleichung

$$4^n \leq (2n)^{1+\sqrt{2n}} \cdot 4^{2n/3}$$

was äquivalent ist zu

$$4^{n/3} \leq (2n)^{1+\sqrt{2n}}$$

und (Potenzieren der Ungleichung mit 3)

$$2^{2n} \leq (2n)^{3(1+\sqrt{2n})} \qquad (**)$$

Diese Ungleichung ist aber falsch für n ab einer bestimmten Größe! Dies läßt sich zeigen indem man die Abschätzung $n + 1 < 2^n$ für $n \geq 2$ benutzt.

[3] Das erste Produkt läßt sich mit dieser Abschätzung jedoch nicht erschlagen, da über $2n$ multipliziert wird (da auch Potenzen der Primzahlen auftreten können).

Beweis:
IA: $n = 2$ also $3 < 2^2$ was stimmt.
IS: $(n+1)+1 < 2^{n+1}$ was sich nach IV abschätzen lässt zu $2^n+1 < 2\cdot 2^n = 2^n+2^n$ oder $1 < 2^n$ was für alle n stimmt.

Nach dieser Abschätzung (beim zweiten $<$) gilt

$$2n = (\sqrt[6]{2n})^6 < \left(\lfloor\sqrt[6]{2n}\rfloor + 1\right)^6 < 2^{6\lfloor\sqrt[6]{2n}\rfloor} \leq 2^{6\sqrt[6]{2n}}$$

Damit läßt sich die rechte Seite der Ungleichung (∗∗) abschätzen zu

$$(2n)^{3(1+\sqrt{2n})} < 2^{6\sqrt[6]{2n}\cdot 3(1+\sqrt{2n})} = 2^{\sqrt[6]{2n}(18+18\sqrt{2n})}$$

Für $n \geq 50$ gilt nun die Abschätzung $18 < 2\sqrt{2n}$ wodurch man hier die erste 18 ersetzt[4], also

$$< 2^{\sqrt[6]{2n}\cdot 20\sqrt{2n}} = 2^{20(2n)^{2/3}}$$

Vergleicht man dies nun mit der linken Seite von Ungleichung (∗∗) so müsste (für die Exponenten) gelten

$$2n < 20(2n)^{2/3} \quad\Leftrightarrow\quad (2n)^{1/3} < 20 \quad\Leftrightarrow\quad n < 4000$$

Für $n \geq 4000$ muss BERTRANDS Postulat also stimmen, da sich sonst ein Widerspruch ergibt! Für $n < 4000$ wurde der Beweis bereits in Teil (1) geführt.

Damit ist BERTRANDS Postulat für alle $n \in \mathbb{N}$ bewiesen. □

Anhang

Aus der Ungleichung am Ende von Schritt 4 lässt sich auch ableiten, dass gilt:

$$\prod_{n<p\leq 2n} p \geq 2^{n/30} \quad \text{für} \quad n \geq 30000$$

Da die einzelnen Primzahlen kleiner gleich $2n$ sind muss es also mindestens $\log_{2n}(2^{\frac{1}{30}n})$ von ihnen geben. Zwischen n und $2n$ gibt es also mindestens

$$\log_{2n}(2^{\frac{1}{30}n}) = \frac{n}{30}\cdot\log_{2n} 2 = \frac{n}{30}\cdot\frac{1}{\log_2 2n} = \frac{1}{30}\cdot\frac{n}{1+\log_2 n}$$

Primzahlen. Für sehr große n kann man die 1 im Nenner vernachlässigen und erhält so

$$\frac{1}{30}\frac{n}{\log_2 n} \approx 0,023\cdot\frac{n}{\log n}$$

Eigentlich ist das kein so schlechter Wert, denn die echte Anzahl beträgt ungefähr $\frac{n}{\log n}$. Dies folgt aus dem Primzahlentheorem, das lautet

$$\lim_{n\to\infty}\frac{\#\{p \leq n \,|\, p \text{ Primzahl}\}}{\frac{n}{\log n}} = 1$$

Die Anzahl der Primzahlen zwischen n und $2n$ wäre hier nach ungefähr

$$\frac{2n}{\log 2n} - \frac{n}{\log n} = \frac{2n}{\log 2 + \log n} - \frac{n}{\log n}$$

Für sehr große n kann man $\log 2$ vernachlässigen, so dass man $\frac{n}{\log n}$ erhält.

Eine BERTRANDS Postulat ähnliche Aussage ist ein noch ungelöstes Problem. Sie lautet

Für jedes $n \in \mathbb{N}$ existiert eine Primzahl p mit $n^2 < p < (n+1)^2$.

[4]Zum Beweis setzte einfach für $n = 50$ ein (Monotonie der Wurzel), was $18 < 2\sqrt{100} = 20$ ergibt.