Bertrands Postulat

Ingolf Giese

Februar 2018

1 Behauptung

Zu jeder ganzen Zahl $n > 0$ gibt es (mindestens) eine Primzahl p mit

$$n < p \leq 2n$$

$\Rightarrow$ Daraus folgt auch: Es gibt unendlich viele Primzahlen.

Dieses Postulat wurde 1845 von Joseph Bertrand (mit 23 Jahren) aufgestellt (und für alle Zahlen bis 3000000 bewiesen), aber erstmals 1850 von Pafnuti L. Tschebyschow (P. L. Tchebychef) bewiesen. Den ersten relativ elementaren Beweis fand Srinivasa Ramanujan 1919, er benutzt dabei aber verschiedene Primzahlfunktionen und die Stirling-Formel.

1932 fand Paul Erdős (mit 19 Jahren) einen eleganten und elementaren Beweis, der hier im Wesentlichen dargestellt wird (siehe https://users.renyi.hu/~p_erdos/1932-01.pdf).

2 Beweis-Idee

Erdős benutzte zwei grundlegende Ideen:
Zuerst betrachtet man das Produkt aller Primzahlen p zwischen n und $2n$ (für ein gegebenes n):

$$\prod_{n<p\leq 2n} p$$

Ist das Produkt größer als 1, gibt es im Bereich $n < p \leq 2n$ mindestens eine Primzahl; liegt dort jedoch keine Primzahl, ist das Produkt gleich 1.

Die zweite Idee ist, die mittlere Zahl (Binomialkoeffizient) einer geradzahligen Reihe im Pascalschen Dreieck, also $\binom{2n}{n}$, als Produkt aller vorhandenen Primzahlen zu schreiben. Dabei tritt das obige Produkt auf und durch geschickte Abschätzungen kann das Postulat bewiesen werden (vp Vielfachheit von p in $\binom{2n}{n}$):

$$\ldots \leq \binom{2n}{n} = \prod_{p\leq\sqrt{2n}} p^{vp} \cdot \ldots \cdot \prod_{n<p\leq 2n} p$$

3 Beweis

Wegen der im Folgenden oft groben Abschätzungen sei n genügend groß.

Untersuchung der mittleren Zahl (Binomialkoeffizient) einer geradzahligen Reihe im Pascalschen Dreieck:

$$(1) \qquad \binom{2n}{n} = \frac{(2n)!}{n! \cdot n!} = \frac{(n+1) \cdot (n+2) \cdot \ldots \cdot (2n)}{1 \cdot 2 \cdot \ldots \cdot n}$$

Beispiel: Pascalsches Dreieck mit 7 Reihen:

k=0							1						
k=1						1		1					
k=2					1		2		1				
k=3				1		3		3		1			
k=4			1		4		6		4		1		
k=5		1		5		10		10		5		1	
k=6	1		6		15		20		15		6		1

Abschätzung nach unten:

Die Summe aller Zahlen der $(2n)$-ten Reihe im Pascalschen Dreieck ist 4^n wegen:

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

Der Mittelwert aller Zahlen dieser Reihe (wobei man hier die erste und letzte Zahl mit den Werten 1 zusammenfasst) ist daher der $(2n)$-te Teil, und da der mittlere Binomialkoeffizient $\binom{2n}{n}$ die größte Zahl der Reihe ist, folgt:

$$(2) \qquad \frac{4^n}{2n} \le \binom{2n}{n}$$

PS: Es sind auch bessere Abschätzungen, z.B. mit $\frac{4^n}{n}$ bzw. $1.5 \cdot \frac{4^n}{n}$ (ab $n = 8$), möglich.

Primzahlzerlegung von $\binom{2n}{n}$:

PS: Es wird immer davon ausgegangen, dass es Primzahlen geben könnte: $q < p \le r$ heißt also genauer "falls es p gibt mit $q < p \le r$".

Die größte auftretende Primzahl von $\binom{2n}{n} = \frac{(2n)!}{n! \cdot n!}$ ist maximal $2n$ (siehe Gleichung (1)), also geht das folgende Produkt nur bis $2n$:

$$(3) \qquad \binom{2n}{n} = \prod_p p^{vp} = \prod_{p \le 2n} p^{vp}$$

Dabei sind die p alle Primzahlen (bis $2n$) und vp ist die Vielfachheit der Primzahl p im Binomialkoeffizienten $\binom{2n}{n}$, also $vp = v_p(\binom{2n}{n})$.

Wesentliche Idee:

Aufteilung in vier Bereiche (mit mindestens $n \geq 5$, damit $\sqrt{2n} < \frac{2}{3}n$ gilt):

(4) $$\binom{2n}{n} = \prod_{p \leq \sqrt{2n}} p^{vp} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p^{vp} \cdot \prod_{\frac{2}{3}n < p \leq n} p^{vp} \cdot \prod_{n < p \leq 2n} p^{vp}$$

Beispiel: Zerlege mit $n = 18$ den Binomialkoeffizienten $\binom{36}{18}$ also in die 4 Bereiche:

$$p \leq 6, \quad 6 < p \leq 12, \quad 12 < p \leq 18, \quad 18 < p \leq 36 :$$

$$\binom{36}{18} = (2^2 \cdot 3 \cdot 5^2) \cdot (7 \cdot 11) \cdot (13^0 \cdot 17^0) \cdot (19 \cdot 23 \cdot 29 \cdot 31) = 9075135300$$

Hilfssatz: Identität von Legendre:

(5) $n!$ enthält den Primfaktor p genau $\displaystyle\sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$ Mal

PS: Die Schreibung $\lfloor x \rfloor$ bedeutet floor(x), also der ganzzahlige Anteil von x ($x \geq 0$).

Beweis: Genau $\lfloor \frac{n}{p} \rfloor$ der Faktoren von $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ sind durch p teilbar. Davon sind $\lfloor \frac{n}{p^2} \rfloor$ sogar durch p^2 teilbar, $\lfloor \frac{n}{p^3} \rfloor$ durch p^3, usw..

Wegen $\binom{2n}{n} = \frac{(2n)!}{n! \cdot n!}$ gilt mit der obigen Definition von vp:

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

Daraus folgt wegen $p^k \leq 2n$ und vp ganzzahlig:

(6) Die Primzahlen p mit $\sqrt{2n} < p \leq 2n$ sind höchstens 1 Mal in $\binom{2n}{n}$ enthalten

Abschätzungen nach oben:

Das **erste Produkt**, bei dem im Allgemeinen Vielfachheiten größer als 1 auftreten, wird einfach grob abgeschätzt durch die maximal mögliche Primzahl $2n$.
Zusatz zu dem Beweis von Erdős (mit $\sqrt{2n}$ Faktoren): Da 1 keine Primzahl ist, sind das maximal $\sqrt{2n} - 1$ Faktoren:

(7) $$\prod_{p \leq \sqrt{2n}} p^{vp} \leq \prod_{p \leq \sqrt{2n}} (2n) \leq (2n)^{\sqrt{2n}-1}$$

PS: Man kann die Anzahl auch mit $\pi(n) \leq \frac{1}{3}n + 2$, $\frac{4}{15}n + 3$ oder $1.26 \cdot \frac{n}{log(n)}$ abschätzen.

Das **zweite Produkt** enthält nach Gleichung (6) nur die Vielfachheiten 0 oder 1 und wird grob abgeschätzt durch den Hilfssatz $\prod_{p \leq x} p \leq 4^{x-1}$ (Beweis siehe Anhang), wobei die Ungleichung weiter vergrößert wird:

(8) $$\prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p^{vp} \leq \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \leq 4^{\frac{2}{3}n-1} < 4^{\frac{2}{3}n}$$

Für das **dritte Produkt** kann man das zunächst erstaunliche Resultat zeigen, dass alle Vielfachen 0 sind - das ist der springende Punkt dieses Beweises.
Denn: Wegen $\frac{2}{3}n < p$ ist $3p > 2n$, d.h. die mindestens 3-fachen einer Primzahl sind oberhalb von $2n$. Damit kann p in der Primfaktorzerlegung von $\binom{2n}{n}$ maximal 2 Mal im Zähler auftreten, wird aber wegen $p \leq n$ auch 2 Mal im Nenner gekürzt, also folgt:

$$(9) \qquad \prod_{\frac{2}{3}n<p\leq n} p^{vp} = \prod_{\frac{2}{3}n<p\leq n} p^0 = 1$$

PS: Weitere Löcher (mit $vp = 0$) liegen bei $\frac{2}{5}n < p \leq \frac{n}{2}$, $\frac{2}{7}n < p \leq \frac{n}{3}$, $\frac{2}{9}n < p \leq \frac{n}{4}$, ...

Für das **vierte Produkt** folgt, da kein Primfaktor von $\binom{2n}{n} = \frac{(2n)!}{n!\cdot n!}$ gekürzt werden kann (wegen $p > n$), und wegen der Vielfachheit 1 - siehe Gleichung (6):

$$(10) \qquad \prod_{n<p\leq 2n} p^{vp} = \prod_{n<p\leq 2n} p$$

Bertrands Postulat besagt, dass das rechts stehende Produkt größer als 1 ist.

Beweis: Insgesamt hat man jetzt aus den Gleichungen (2) und (3) mit den vier Produkten aus den Gleichungen (7) bis (10) und mit (mindestens) $n \geq 5$:

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

Umgeformt folgt daraus (gegenüber Erdős ohne störende $+1$ in den Exponenten):

$$(11) \qquad Q = \frac{4^{\frac{1}{3}n}}{(2n)^{\sqrt{2n}}} < \prod_{n<p\leq 2n} p$$

Hier sieht man schon ohne genauere Rechnung, dass ab einem bestimmten n der Quotient $Q > 1$ ist, da 4^n wesentlich stärker wächst als etwa $z^{\sqrt{n}}$, auch wenn n in der Basis z auftritt (was man durch die Identität $2n = 2^{\log[2](2n)}$ leicht beheben könnte).

Zur genaueren Analyse untersucht man, ob es wirklich ein n gibt, ab dem der Quotient Q größer als 1 ist, d.h.:

$$1 < Q = \frac{4^{\frac{1}{3}n}}{(2n)^{\sqrt{2n}}} = \frac{2^{\frac{1}{3}(2n)}}{(2n)^{\sqrt{2n}}}$$

$(2n)$ im Exponenten des Zählers geschrieben als $\sqrt{2n} \cdot \sqrt{2n}$ ergibt:

$$1 < \frac{2^{\frac{1}{3}\sqrt{2n}\cdot\sqrt{2n}}}{(2n)^{\sqrt{2n}}}$$

oder umgeformt:

$$1 < \frac{(2^{\frac{1}{3}\sqrt{2n}})^{\sqrt{2n}}}{(2n)^{\sqrt{2n}}} = \left(\frac{2^{\frac{1}{3}\sqrt{2n}}}{2n}\right)^{\sqrt{2n}}$$

Wegen $1 = 1^{1/\sqrt{2n}}$ erhält man durch Potenzieren die zu $1 < Q$ äquivalente Ungleichung:

$$(12) \qquad 1 \;<\; \frac{2^{\frac{1}{3}\sqrt{2n}}}{2n} \;=\; Q^{1/\sqrt{2n}}$$

Das schnellere Wachstum des Zählers gegenüber dem Nenner sieht man insbesondere beim Betrachten bestimmter Werte von n:

Mit $n = 18 \cdot M^2$ und $M = 1, 2, 3, 4, 5, \ldots$ folgt aus Gleichung (12):

$$1 \;<\; \frac{2^{2M}}{36 \cdot M^2} \;=\; \left(\frac{2^M}{6 \cdot M}\right)^2$$

Das zeigt, dass der Zähler wesentlich schneller wächst als der Nenner, wegen der auftretenden Faktoren hier ab $M = 5$, also $n = 450$:

$$M = 4 \leftrightarrow n = 288 \qquad \left(\frac{2^M}{6 \cdot M}\right)^2 \;=\; \left(\frac{16}{24}\right)^2 \;=\; \frac{256}{576} \;=\; 0.44444444444444$$

$$M = 5 \leftrightarrow n = 450 \qquad \left(\frac{2^M}{6 \cdot M}\right)^2 \;=\; \left(\frac{32}{30}\right)^2 \;=\; \frac{1024}{900} \;=\; 1.1377777777778$$

Und damit folgt insgesamt aus den Gleichungen (11) und (12):

$$(13) \qquad \prod_{n<p\leq 2n} p > 1$$

Damit ist Bertrands Postulat für alle $n \geq 450$ bewiesen.

Die Richtigkeit des Postulats zeigt man für die kleineren n mit dem so genannten Landau-Trick: Man schreibt bestimmte Primzahlen in einer Folge auf:
2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 5003, ...

Dabei sieht man, da jedes Folgenglied kleiner als das Doppelte des vorhergehenden ist, dass auch für $n < 450$ das Bertrandsche Postulat gilt.

P.S.: Ausführliche Computer-Rechnungen zeigen, dass der Quotient Q aus Gleichung (11) schon ab $n = 427$ größer als 1 ist und danach, wie zu erwarten, rasant ansteigt:

$$n = 427 : \frac{4.9340714290321E + 85}{4.6431151112854E + 85} \;=\; 1.0626640328256$$

$$n = 441 : \frac{3.1828687130226E + 88}{2.9919479459571E + 87} \;=\; 10.638115269764$$

$$n = 455 : \frac{2.0532036047816E + 91}{1.8325379057109E + 89} \;=\; 112.04153531466$$

$$n = 468 : \frac{8.3436993590661E + 93}{8.0086847362466E + 90} \;=\; 1041.8314160006$$

PS: Der Originalbeweis von Erdős benutzt einen komplizierteren Trick zum Umformen des Quotienten Q mit Hilfe der 6-ten Wurzel und der floor-Funktion:

$$2n \;=\; ((2n)^{1/6})^6 \;<\; (\lfloor (2n)^{1/6} \rfloor + 1)^6$$

Das ist aber wegen $(k+1) \leq 2^k$ kleiner oder gleich

$$\leq \; 2^{6\cdot\lfloor(2n)^{1/6}\rfloor} \; \leq \; 2^{6\cdot(2n)^{1/6}}$$

Damit wird die Basis $(2n)$ im Nenner von Q, im Originalbeweis $Q = \dfrac{4^{\frac{1}{3}n+1}}{(2n)^{\sqrt{2n}+1}}$, von n unabhängig gemacht. Im Beweis selbst wird angenommen, dass das Postulat falsch ist, also $Q \leq 1$ unterstellt wird. Das heißt (da $18 < 2 \cdot \sqrt{2n}$ für $n \geq 41$ gilt):

$$2^{2n} \; < \; 2^{2n+6} \; = \; (4^{\frac{1}{3}n+1})^3 \; \leq \; ((2n)^{\sqrt{2n}+1})^3 \; < \; 2^{18\cdot(2n)^{\frac{1}{6}}(\sqrt{2n}+1)} \; < \; 2^{20\cdot(2n)^{\frac{2}{3}}}$$

Durch Logarithmieren wird dann abgeleitet, dass daraus $n < 4000$ folgt. Damit gilt der Beweis des Bertrandsche Postulats aber für $n \geq 4000$. Weil aber mittels des Landau-Tricks das Postulat auch für $n < 4000$ richtig ist, gilt Bertrands Postulat für alle n.

4 Anhang

Induktionsbeweis von (bei $x \geq 2$, p Primzahl):

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

Der Induktionsanfang ist trivial, sei also die Behauptung bewiesen bis $x = 2m$. Dann gilt für $x = 2m+1$:

$$\prod_{p \leq 2m+1} p \; = \; \prod_{p \leq m+1} p \; \cdot \prod_{m+1 < p \leq 2m+1} p \; \leq \; 4^m \; \cdot \prod_{m+1 < p \leq 2m+1} p \tag{14}$$

Induktionsbeweis: Es gilt nach dem binomischen Lehrsatz, durch Weglassen der kleineren Summanden und wegen der Gleichheit der beiden mittleren Terme:

$$2 \cdot 4^m \; = \; 2^{2m+1} \; = \; (1+1)^{2m+1} \; = \; \sum_{k=0}^{2m+1} \binom{2m+1}{k} \; \geq \; 2 \cdot \binom{2m+1}{m}$$

Daraus erhält man:

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

Für das letzte Produkt in Gleichung (14) gilt daher, weil alle Primfaktoren $m+1 < p \leq 2m+1$ im Zähler des Binomschen Ausdrucks enthalten sind und nicht gekürzt werden können:

$$\prod_{m+1 < p \leq 2m+1} p \; \leq \; \frac{(2m+1)!}{m! \cdot (m+1)!} \; = \; \binom{2m+1}{m} \; \leq \; 4^m$$

Insgesamt folgt damit genau die Induktionsbehauptung:

$$\prod_{p \leq 2m+1} p \; = \; \prod_{p \leq m+1} p \; \cdot \prod_{m+1 < p \leq 2m+1} p \; \leq \; 4^m \cdot 4^m \; = \; 4^{2m}$$

PS: Mögliche Verbesserung mit $\prod p \; \leq \; \frac{1}{2} \cdot 4^{x-1}$, eventuell sogar $\leq \; 3^{x-1}$ (nicht $\leq \; e^{x-1}$), wobei die letzten beiden Abschätzungen bis $x = 100$ Millionen gerechnet und auf 100 Milliarden hochgerechnet wurden.

mactex-2016/pdflatex → http://www.sarahandrobin.com/ingo/bertrands-postulat.pdf, http://www.sarahandrobin.com/ingo/index.html