Wiederholung

Satz 2.11 (Tschebyscheff): $\forall n \in \mathbb{N}$ gilt

$$\frac{1}{4}\frac{n}{\ln(n)} \leq \pi(n) \leq 6\frac{n}{\ln(n)}$$

Bemerkung: $2^n < \binom{2n}{n} < 4^n$ für $n > 1$

so gilt auch $\quad n\ln(2) < \ln((2n)!) - 2\ln(n!) < 2n\ln(2) \qquad (1)$

Def: $\nu_p(n)$ bezeichnet die größte Zahl m sodass $p^m | n$

also den Exponent von p in der Primfaktorzerlegung

$$n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}$$

Beweis: Es gilt

$$\nu_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + \ldots$$

wie viele sind durch p teilbar

wie viele sind durch p^2 teilbar

$$= \sum_{m \geq 1} \lfloor \frac{n}{p^m} \rfloor$$

Es ist aber $\lfloor \frac{n}{p^m} \rfloor = 0 \iff p^m > n$

$$\iff m\ln(p) > \ln(n)$$

$$\iff m > \frac{\ln(n)}{\ln(p)}$$

Also ist $\nu_p(n!) = \sum_{m=1}^{\lfloor \frac{\ln(n)}{\ln(p)} \rfloor} \lfloor \frac{n}{p^m} \rfloor$

Daraus folgt

$$\ln((2n)!) - 2\ln(n!) = \ln\left(\prod_{p\in\mathbb{P}} p^{\nu_p((2n)!)}\right) - 2\ln\left(\prod_{p\in\mathbb{P}} p^{\nu_p(n!)}\right)$$

$$= \sum_{p\in\mathbb{P}} \left(\nu_p((2n)!)\ln(p)\right) - 2\sum_{p\in\mathbb{P}}\left(\nu_p(n!)\ln(p)\right)$$

$$= \sum_{\substack{p\in\mathbb{P}\\ p\le 2n}} \left(\sum_{m=1}^{\left\lfloor\frac{\ln(2n)}{\ln(p)}\right\rfloor} \left\lfloor \frac{2n}{p^m}\right\rfloor - 2\sum_{m=1}^{\left\lfloor\frac{\ln(n)}{\ln(p)}\right\rfloor} \left\lfloor\frac{n}{p^m}\right\rfloor \right)\ln(p)$$

$$= \sum_{\substack{p\in\mathbb{P}\\ p\le 2n}} \left(\sum_{m=1}^{\left\lfloor\frac{\ln(2n)}{\ln(p)}\right\rfloor} \left(\left\lfloor \frac{2n}{p^m}\right\rfloor - 2\left\lfloor\frac{n}{p^m}\right\rfloor \right)\ln(p)\right) \qquad (1,5)$$

Es ist $\lfloor 2x\rfloor - 2\lfloor x\rfloor = \begin{cases} 0 & \text{wenn } x - \lfloor x\rfloor < \frac{1}{2} \\ 1 & \text{wenn } x - \lfloor x\rfloor \ge \frac{1}{2} \end{cases}$

also folgt

$$\ln((2n)!) - 2\ln(n!) \le \sum_{\substack{p\in\mathbb{P}\\ p\le 2n}} \sum_{m=1}^{\left\lfloor\frac{\ln(2n)}{\ln(p)}\right\rfloor} 1\cdot\ln(p)$$

$$= \sum_{\substack{p\in\mathbb{P}\\ p\le 2n}} \left\lfloor\frac{\ln(2n)}{\ln(p)}\right\rfloor \ln(p) \qquad (2)$$

Aus (1) und (2) folgt

$$n \ln(2) < \sum_{\substack{p \in \mathbb{P} \\ p \leq 2n}} \left\lfloor \frac{\ln(2n)}{\ln(p)} \right\rfloor \ln(p)$$

$$\leq \sum_{\substack{p \in \mathbb{P} \\ p \leq 2n}} \ln(2n)$$

$$= \pi(2n) \ln(2n)$$

Also ist $\pi(2n) > \frac{n \ln(2)}{\ln(2n)}$

$$> \frac{1}{4} \frac{2n}{\ln(2n)} \qquad \left(\ln(2) > \tfrac{1}{2}\right)$$

untere Schranke für gerade Zahlen

Und $\pi(2n+1) \geq \pi(2n) > \frac{n \ln(2)}{\ln(2n)}$

$$= \frac{2n+1}{\ln(2n+1)} \cdot \frac{\ln(2n+1)}{\ln(2n)} \cdot \frac{n \ln(2)}{2n+1}$$

$$> \frac{2n+1}{\ln(2n+1)} \cdot 1 \cdot \frac{1}{4}$$

$$= \frac{1}{4} \cdot \frac{2n+1}{\ln(2n+1)}$$

untere Schranke für ungerade Zahlen.

Die untere Schranke ist damit bewiesen

Wir definieren $\theta(x) := \sum_{\substack{p \in \mathbb{P} \\ p \leq x}} \ln(p)$

$\forall p \in \mathbb{P}$ mit $n < p < 2n$ ist $\lfloor \frac{2n}{p} \rfloor - 2 \lfloor \frac{n}{p} \rfloor = 1 - 0 = 1$

Also gilt

$$\begin{aligned}
\theta(2n) - \theta(n) &= \sum_{\substack{p \in \mathbb{P} \\ n < p \leq 2n}} \ln(p) \\
&= \sum_{\substack{p \in \mathbb{P} \\ n < p \leq 2n}} \left(\lfloor \tfrac{2n}{p} \rfloor - 2 \lfloor \tfrac{n}{p} \rfloor \right) \ln(p) \\
&= \sum_{\substack{p \in \mathbb{P} \\ n < p \leq 2n}} \sum_{m=1}^{\lfloor \frac{\ln(2n)}{\ln(p)} \rfloor} \left(\lfloor \tfrac{2n}{p^m} \rfloor - 2 \lfloor \tfrac{n}{p^m} \rfloor \right) \ln(p) \\
&\leq \ln((2n)!) - 2\ln(n!) \qquad \text{(aus (1,5))} \\
&< 2n \ln(2) \qquad \text{(aus (1))}
\end{aligned}$$

Insbesondere gilt

$$\theta(2^{r+1}) - \theta(2^r) < 2^{r+1} \ln(2)$$

Also gilt

$$\begin{aligned}
\theta(2^{r+1}) &= \sum_{i=0}^{r} \left(\theta(2^{i+1}) - \theta(2^i) \right) + \theta(2^0) \\
&< \sum_{i=0}^{r} 2^{i+1} \ln(2) + 0 \\
&< 2^{r+2} \ln(2) \qquad (3)
\end{aligned}$$

: Sei $2^k \leq n < 2^{k+1}$ und $y < n$

Dann gilt
$$
\begin{aligned}
(\pi(n) - \pi(y)) \ln(y) &= \sum_{\substack{p \in \mathbb{P} \\ y < p \leq n}} \ln(y) \\
&< \sum_{\substack{p \in \mathbb{P} \\ y < p \leq n}} \ln(p) \\
&= \theta(n) - \theta(y) \\
&\leq \theta(n) \\
&\leq \theta(2^{k+1}) \\
&< 2^{k+2} \ln(2) \qquad (\text{aus } (3)) \\
&\leq 4n \ln(2)
\end{aligned}
$$

Wähle nun $y := n^{2/3}$

und da $\pi(y) \leq y = n^{2/3}$, gilt
$$
\begin{aligned}
\pi(n) &< \frac{4n\ln(2)}{\ln(y)} + \pi(y) \\
&\leq \frac{4n\ln(2)}{\frac{2}{3}\ln(n)} + n^{2/3} \\
&= \frac{n}{\ln(n)}\left(6\ln(2) + n^{-1/3}\ln(n)\right)
\end{aligned}
$$

Sei $f(x) = x^{-1/3} \ln(x)$

$$f'(x) = \frac{-1}{3} x^{-4/3} \ln(x) + x^{-1/3} \cdot x^{-1}$$
$$= x^{-4/3} \left(\frac{-1}{3} \ln(x) + 1 \right)$$

$$f'(x) = 0 \iff \frac{1}{3} \ln(x) = 1$$
$$\iff \ln(x) = 3$$
$$\iff x = e^3$$

das heisst f erreicht sein Maximum bei $x = e^3$

Also $$\pi(n) < \frac{n}{\ln(n)} \left(6 \ln(2) + \frac{\ln(e^3)}{(e^3)^{1/3}} \right)$$
$$= \frac{n}{\ln(n)} \left(6 \ln(2) + \frac{3}{e} \right)$$
$$< 6 \frac{n}{\ln(n)}$$

$\square$

Vermutungen über Primzahlen

Die Goldbachsche Vermutung:

(1) Jede gerade Zahl $n > 2$ ist als Summe zweier Primzahlen darstellbar:

$$n = p + q \quad , \quad p, q \in \mathbb{P}$$

Warum ist das plausibel?

n hat $\simeq \frac{n}{2}$ verschiedene Darstellungen $n = a + (n-a)$, $a \in \{2, 3, \dots \lfloor \frac{n}{2} \rfloor\}$

eigentlich keine Zufallsvariable

Die Wahrscheinlichkeit, dass $m \in \mathbb{P}$ ist

$$\sim \frac{d}{dm} \frac{m}{\ln(m)} = \frac{1}{\ln(m)} + m \cdot \frac{1}{m} \cdot \frac{-1}{(\ln(m))^2}$$

$$\sim \frac{1}{\ln(m)}$$

Die Wahrscheinlichkeit, dass $a, n-a \in \mathbb{P}$ ist $\sim \frac{1}{\ln(a)} \cdot \frac{1}{\ln(n-a)}$

GELOGEN!
(nicht unabhängig)

Erwartete Anzahl Darstellungen mit Primzahlen ist

$$\sum_{i=2}^{\lfloor n/2 \rfloor} \frac{1}{\ln(i)} \frac{1}{\ln(n-i)} \gtrsim \frac{n}{2} \cdot \frac{1}{(\ln(n/2))^2}$$

$$\rightarrow \infty$$

würde immer noch nicht beweisen, dass jede Zahl mindestens eine Darstellung hat.

Die Vermutung gilt für alle $n \leq 2 \cdot 10^{17}$

(2) Jede ungerade Zahl $n > 7$ ist als Summe dreier ungerader Primzahlen darstellbar:

$$n = p + q + r \quad , \quad p, q, r \in \mathbb{P} \setminus \{2\}$$

Gilt für n groß, d.h. $n \geq 2 \cdot 10^{1346}$

Def: <u>Primzahlzwillinge</u> sind Zahlen der Form $p, p+2$
wobei $p, p+2 \in \mathbb{P}$

$(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, ...

Vermutung: Es gibt unendlich viele Primzahlzwillinge

Vermutung (de Polignac): $\forall k \in \mathbb{N}$ gibt es unendlich viele Zahlen p sodass $p, p+2k \in \mathbb{P}$

Der Fall $k=1$ ist die Vermutung über Primzahlzwillinge

Diese Vermutung ist bisher für <u>keine</u> Zahl k bewiesen oder widerlegt worden.