Elementare Primzahlverteilung

Ausarbeitung zum Seminar
Funktionentheorie

Vortrag 02. 04. 2012

Sara Bohmann

§1 Einleitung

Ziel des ersten Blocks des Seminars zur Funktionentheorie ist der sogenannte Primzahlsatz. Dieser erlaubt eine endliche Abschätzung der Verteilung der Primzahlen mittels Logarithmen. Der Zusammenhang zwischen Primzahlen und Logarithmen wurde bereits im Jahre 1793 von dem damals 15-jährigen Carl Friedrich Gauß und unabhängig von ihm im Jahre 1798 durch Adrien-Marie Legendre vermutet, aber erst 1896 von Jacques Salomon Hadamard und Charles-Jean de La Vallée Poussin bewiesen.
Genauer zitiert, besagt der Primzahlsatz, dass die Anzahl der Primzahlen kleiner gleich einer Zahl x (bez. mit $\pi(x)$) durch $\frac{x}{\ln(x)}$ angenähert werden kann.
Mathematisch exakt:

$$\pi(x) \sim \frac{x}{\ln(x)}$$

(gesprochen "x und $\frac{x}{\ln(x)}$ sind asymptotisch gleich") mit

(1.1) Definition
Seien $f, g, h : [a, \infty) \to \mathbb{C}$ Funktionen. Man schreibt

$$f(x) = \mathcal{O}(h(x)) \text{ (für } x \geq a),$$

wenn es ein $C > 0$ gibt, sodass

$$|f(x)| \leq C \cdot |h(x)| \text{ (für alle } x \geq a).$$

Die Gleichung

$$f(x) = g(x) + \mathcal{O}(h(x))$$

ist gleichbedeutend mit $f(x) - g(x) = \mathcal{O}(h(x))$.
Man nennt $\mathcal{O}$ das Landau*sche Oh-Symbol*.
Gilt

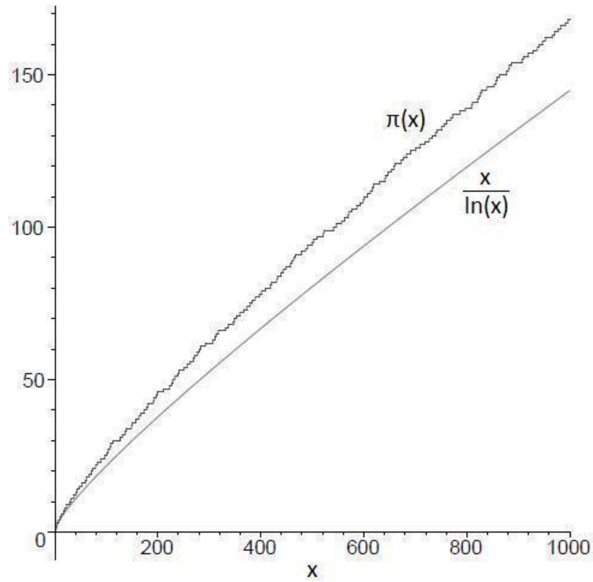
$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1,$$

so schreibt man

$$f(x) \sim g(x) \text{ (für } x \to \infty)$$

und nennt $f(x)$ und $g(x)$ *asymptotisch gleich*.

Bildlich lässt sich der Primzahlsatz folgendermaßen verdeutlichen:



In dieser Ausarbeitung sollen zunächst grundlegende Begriffe definiert werden und erste Aussagen über die Verteilung von Primzahlen gemacht werden, die zum Beweis des Primzahlsatzes führen.
Die gängige Definition einer Primzahl lautet:
$p \in \mathbb{N}, p > 1$ ist eine *Primzahl*, wenn gilt: $n|p,\ n \in \mathbb{Z} \Leftrightarrow n \in \{\pm 1, \pm p\}$.
Äquivalent zu dieser Definition ist auch die folgende:
$p \in \mathbb{N}$ ist eine *Primzahl*, wenn $p > 1$ und $p|m \cdot n,\ m, n \in \mathbb{Z} \Rightarrow p|m$ oder $p|n$ gilt.
Dabei verwendet wurde auch der bereits bekannte Teilbarkeitsbegriff:
$a, b \in \mathbb{Z}, a \mid b \Leftrightarrow \exists c \in \mathbb{Z} : ac = b$.

Verwenden wollen wir auch folgende

(1.2) Bezeichnung
Mit $\mathbb{P}$ bezeichnen wir die Menge der Primzahlen,

$$\mathbb{P} = \{2, 3, 5, 7, 11, ...\}$$

Mit $(p_n)_{n \geq 1}$ bezeichnen wir die streng monoton wachsende Folge aller Primzahlen, also

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \quad p_4 = 7, \quad p_5 = 11, \quad ...$$

Die *Primzahlzählfunktion* definieren wir als

$$\pi(x) := |\{p \in \mathbb{P}; p \leq x\}| \ , \ x \in \mathbb{R}.$$

§2 Elementare Primzahlverteilung

Ohne Beweis notieren wir den

(1.3) Fundamentalsatz der Arithmetik
Jedes $n \in \mathbb{N}$ besitzt eine eindeutige Darstellung der Form

$$n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}, \quad \nu_p(n) \in \mathbb{N}_0, \quad \nu_p(n) = 0 \text{ für fast alle } p.$$

Diese Darstellung der Zahl $n \in \mathbb{N}$ bezeichnen wir als *Primfaktorzerlegung* von n. $\nu_p(n)$ heißt die *Vielfachheit* von p in n.

Bekannt ist der

(1.4) Satz von EUCLID
Es gibt unendlich viele Primzahlen.

Beweis.
Angenommen, es gibt nur endlich viele Primzahlen. Diese seien mit $q_1, ..., q_r$ bezeichnet. $q_1 = 2$ kennen wir bereits.
Definiere nun $n := q_1 \cdot ... \cdot q_r + 1$. Dann ist $n > 1$.
Außerdem gilt für alle $1 \leq i \leq r$: $q_i | q_1 \cdot ... \cdot q_r = n - 1$, also $q_i \nmid n$.
Gemäß dem Fundamentalsatz der Arithmetik (1.3) gibt es für n eine Darstellung $n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}$ mit $\nu_p(n) \in \mathbb{N}_0$ und $\nu_p(n) = 0$ für fast alle p. Es gibt also mindestens eine Primzahl, die n teilt. Sei q_{r+1} diese Primzahl. Dann gilt $q_{r+1} \neq q_i$, $i = 1, ..., r$, da diese n nicht teilen. Somit haben wir zusätzlich zu $q_1, ..., q_r$ eine weitere Primzahl q_{r+1} gefunden.
Dies ist ein Widerspruch zur Annahme und somit ist die Aussage gezeigt. $\square$

Betrachten wir die im Beweis von (1.4) konstruierte Folge:
Bekanntlich gilt $q_1 = 2$.
Definiere nun $n := q_1 + 1 = 2 + 1 = 3$. Dann gilt $n = 3 \in \mathbb{P}$, also $q_2 = 3$.
Setze jetzt $n := q_1 \cdot q_2 + 1 = 2 \cdot 3 + 1 = 7$. Dann gilt $n = 7 \in \mathbb{P}$, also $q_3 = 7$.
Genauso entsteht $q_4 = 43$.
Definiere nun $n := q_1 \cdot q_2 \cdot q_3 \cdot q_4 + 1 = 2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807 = 13 \cdot 139$. Nun gilt $n \notin \mathbb{P}$, wobei 13 die kleinste Primzahl ist, die n teilt. Es ergibt sich also $q_5 = 13$.
So kann man natürlich beliebig lang fortfahren. Es ist eine offene Frage, ob auf diese Weise alle Primzahlen entstehen.

Zusätzlich zu der Unendlichkeit der Menge der Primzahlen kennen wir auch noch das

(1.5) Korollar
Es gibt unendlich viele Primzahlen der Form $4k + 3, k \in \mathbb{N}_0$.

Beweis.
Angenommen, es gibt nur endlich viele Primzahlen der Form $4k+3, k \in \mathbb{N}_0$. Diese seien mit $p_1, ..., p_n$ bezeichnet. Definiere $z := 4p_1 \cdot ... \cdot p_n - 1$. Dann hat z die Form $z = 4k + 3$ mit $k = p_1 \cdot ... \cdot p_n - 1 \in \mathbb{N}_0$. Insbesondere ist z ungerade, da $z = 2l + 1$ mit $l = 2k + 1 \in \mathbb{N}_0$. Sei $z = q_1 \cdot ... \cdot q_m$ die Primfaktorzerlegung von z gemäß (1.3). Da z ungerade ist, gilt $q_i \neq 2$ für alle $i \in \{1, ..., m\}$.
Somit haben die q_i die Form $q_i = 4r_i + 1$ mit $r_i \in \mathbb{N}_0$ ($\Leftrightarrow q_i \equiv 1 \pmod 4$) oder $q_i = 4s_i + 3$ mit $s_i \in \mathbb{N}_0$ ($\Leftrightarrow q_i \equiv 3 \pmod 4$). Angenommen, alle q_i hätten die Form $q_i = 4r_i + 1$. Dann gilt $q_i \equiv 1 \pmod 4$, $i = 1, ..., m \Rightarrow z = q_1 \cdot ... \cdot q_m \equiv 1 \pmod 4$. Dies ist ein Widerspruch. D.h. es gibt ein $\widehat{i} \in \{1, ..., m\}$ mit $q_{\widehat{i}} = 4s_{\widehat{i}} + 3$ für ein $s_{\widehat{i}} \in \mathbb{N}_0$. Dann gilt $q_{\widehat{i}} \in \{p_1, ..., p_n\}$, z.B. $q_{\widehat{i}} = p_j$. Es folgt der Widerspruch

$$p_j = q_{\widehat{i}} \mid q_1 \cdot ... \cdot q_m = z = 4p_1 \cdot ... \cdot p_n - 1. \qquad \square$$

Auch hieraus folgt natürlich die Unendlichkeit der Menge der Primzahlen.

Eine Modifikation der Beweisidee von (1.4) liefert das

(1.6) Lemma
Die Reihe

$$\sum_{p \in \mathbb{P}} \frac{1}{p} = \sum_{k=1}^{\infty} \frac{1}{p_k}$$

divergiert.

Beweis.
Wir führen einen Widerspruchsbeweis und nehmen dazu an, dass die Reihe $\sum\limits_{k=1}^{\infty} \frac{1}{p_k}$ konvergiert. Dann gibt es für jedes $\varepsilon > 0$ ein $N \in \mathbb{N}$, sodass

$$\left| \sum_{k=1}^{n} \frac{1}{p_k} - \sum_{k=1}^{\infty} \frac{1}{p_k} \right| = \left| \sum_{k=1}^{\infty} \frac{1}{p_k} - \sum_{k=1}^{n} \frac{1}{p_k} \right| = \left| \sum_{k=n+1}^{\infty} \frac{1}{p_k} \right| < \varepsilon \text{ für alle } n \geq N.$$

Da $\frac{1}{p_k} > 0$ für jedes $k \geq 1$, existiert somit ein $N \in \mathbb{N}$, sodass

$$\sum_{k>N} \frac{1}{p_k} < \frac{1}{2}. \tag{1}$$

Sei nun $q := p_1 \cdot ... \cdot p_N$. Dann teilt keins der p_i, $i = 1, ..., N$, eine der Zahlen $1 + nq$, $n \in \mathbb{N}$. D.h., dass die Primfaktorzerlegung dieser $1 + nq$, $n \in \mathbb{N}$, nur aus Primfaktoren q_i mit $i > N$ besteht. Also gilt für alle $n \in \mathbb{N}$

$$1 + nq \in M := \{m = \prod_{k=N+1}^{\infty} p_k^{\nu_k};\ \nu_k \in \mathbb{N}_0\ ,\ \nu_k = 0 \text{ für fast alle } k\}.$$

und somit

$$\{1 + nq, n \in \mathbb{N}\} \subseteq M. \tag{2}$$

Für $t \in \mathbb{N}$ gilt mit dem Cauchy-Produkt für Reihen

$$\begin{aligned}
\sum_{\substack{m\in\mathbb{N}, m=p_{i_1}\cdot...\cdot p_{i_t},\\ N<i_1\leq...\leq i_t}} \frac{1}{m} \leq \sum_{m\in\mathbb{N}, m=p_{i_1}\cdot...\cdot p_{i_t}} \frac{1}{m} &= \sum_{(i_1,...,i_t)\in\{N+1,...\}^t} \frac{1}{p_{i_1}\cdot ... \cdot p_{i_t}} \\
&= \sum_{i_1\in\{N+1,...\}} \left(\sum_{i_2\in\{N+1,...\}} \left(... \sum_{i_t\in\{N+1,...\}} \frac{1}{p_{i_1}\cdot ... \cdot p_{i_t}} \right) ... \right) \\
&= \sum_{i_1=N+1}^{\infty} \sum_{i_2=N+1}^{\infty} ... \sum_{i_t=N+1}^{\infty} \frac{1}{p_{i_1}\cdot ... \cdot p_{i_t}} \\
&= \left(\sum_{i_1=N+1}^{\infty} \frac{1}{p_{i_1}} \right) \cdot \left(\sum_{i_2=N+1}^{\infty} \frac{1}{p_{i_2}} \right) \cdot ... \cdot \left(\sum_{i_t=N+1}^{\infty} \frac{1}{p_{i_t}} \right) \\
&= \left(\sum_{k=N+1}^{\infty} \frac{1}{p_k} \right)^t = \left(\sum_{k>N} \frac{1}{p_k} \right)^t
\end{aligned} \tag{3}$$

Daraus ergibt sich für ein $r \in \mathbb{N}$

$$\begin{aligned}
\sum_{n=1}^{r} \frac{1}{1+nq} &\overset{(2)}{\leq} \sum_{m\in M} \frac{1}{m} = \sum_{t=1}^{\infty} \left(\sum_{\substack{m\in\mathbb{N}, m=p_{i_1}\cdot...\cdot p_{i_t},\\ N<i_1\leq...\leq i_t}} \frac{1}{m} \right) \overset{(3)}{\leq} \sum_{t=1}^{\infty} \left(\sum_{k>N} \frac{1}{p_k} \right)^t \\
&\overset{(1)}{\leq} \sum_{t=1}^{\infty} \left(\frac{1}{2} \right)^t = \sum_{t=0}^{\infty} \left(\frac{1}{2} \right)^t - 1 = \frac{1}{1-\frac{1}{2}} - 1 = 1
\end{aligned}$$

Das heißt, die Folge der Partialsummen $(S_r)_{r\geq 1} := \left(\sum_{n=1}^{r} \frac{1}{1+nq} \right)_{r\geq 1}$ ist (monoton wachsend und) nach oben durch 1 beschränkt. Somit folgt

$$\lim_{r\to\infty} S_r \leq 1.$$

Andererseits:
Für $n, q \in \mathbb{N}$ gilt

$$n, q \geq 1 \quad \Rightarrow \quad nq \geq 1 \quad \Rightarrow \quad 2nq \geq 1 + nq \quad \Rightarrow \quad \frac{1}{2nq} \leq \frac{1}{1+nq}$$

und somit mit der Divergenz der harmonischen Reihe

$$\sum_{n=1}^{r} \frac{1}{1+nq} \geq \sum_{n=1}^{r} \frac{1}{2nq} = \frac{1}{2q} \sum_{n=1}^{r} \frac{1}{n}$$
$$\Rightarrow \lim_{r\to\infty} S_r = \lim_{r\to\infty} \sum_{n=1}^{r} \frac{1}{1+nq} \geq \frac{1}{2q} \lim_{r\to\infty} \sum_{n=1}^{r} \frac{1}{n} = \infty.$$

Dies ist ein Widerspruch und somit folgt die Divergenz der Reihe. □

Auch hieraus kann man natürlich folgern, dass es unendlich viele Prinzahlen gibt. Außerdem kann man aus der Konvergenz der Reihe $\sum\limits_{n=1}^{\infty} \frac{1}{n^2}$ schließen, dass es „mehr“ Primzahlen als Quadratzahlen gibt.

Zum Beweis des nächsten Lemmas benötigen wir zunächst folgende

(1.7) Bezeichnung
Für $x \in \mathbb{R}$ bezeichnet $\lfloor x \rfloor := \max\{n \in \mathbb{Z}, n \leq x\}$ die untere Gauss-Klammer.

Anschaulich kann man sich unter $\lfloor \frac{a}{b} \rfloor$ mit $a, b \in \mathbb{N}$ die Anzahl vorstellen, wie oft a von b geteilt wird.
Vergleichen kann man das auch mit der bekannten Division mit Rest: Für $a, b \in \mathbb{N}$ existieren genau ein c und ein $r \in \mathbb{N}$ mit $a = c \cdot b + r$ und $r < b$, nämlich $c = \lfloor \frac{a}{b} \rfloor$ und $r = a - c \cdot b$.
Mit Hilfe der unteren Gaußklammer wollen wir nun die Größenordnung der k-ten Primzahl p_k genauer abschätzen. Dazu zunächst folgendes

(1.8) Lemma
Für alle $n \in \mathbb{N}, 0 \leq j \leq n$ und $p \in \mathbb{P}$ gilt:

a) $\nu_p(n!) = \sum\limits_{k=1}^{\frac{\ln(n)}{\ln(p)}} \lfloor \frac{n}{p^k} \rfloor$

b) $\nu_p(\binom{n}{j}) \leq \frac{\ln(n)}{\ln(p)}$

c) $p^{\nu_p(\binom{n}{j})} \leq n$

d) $\binom{n}{j} \leq n^{\pi(n)}$

e) $2^n \leq \binom{2n}{n} < 4^n$

Beweis.
a) Beachte: Die Vielfachheit $\nu_p(n)$ der Primzahl p in der Primfaktorzerlegung von $n \in \mathbb{N}$ kann auch als Funktion betrachtet werden, durch die n die Anzahl zugeordnet wird, wie oft n von p geteilt wird.
Sei nun zunächst $p > n$: Dann gilt für alle $k \in \mathbb{N}$ die Abschätzung $p^k > n$ und somit $0 < \frac{n}{p^k} < 1$. Also gilt $\lfloor \frac{n}{p^k} \rfloor = 0$ und damit $\sum\limits_{k=1}^{\lfloor \frac{\ln(n)}{\ln(p)} \rfloor} \lfloor \frac{n}{p^k} \rfloor = 0$. Genauso folgt aus $p > n$ auch $p \nmid 1, ..., n$ und somit $p \nmid n!$, also $\nu_p(n!) = 0$ und somit die Behauptung für $p > n$.
Sei nun $p \leq n$: Die Zahl $\nu_p(n!)$ beschreibt die Anzahl, wie oft $n!$ von p geteilt wird. Wegen $n! = 1 \cdot ... \cdot n$ ist dies die Anzahl, wie oft die Zahlen $1, ..., n$ von p geteilt werden. Wir machen also einen Abzählbeweis.
Unter den Zahlen $1, ..., n$ treten die Vielfachen von p in der Form

$$p, 2p, 3p, ..., m_1 p \text{ mit } m_1 = \lfloor \frac{n}{p} \rfloor,$$

$$p^2, 2p^2, 3p^2, ..., m_2 p^2 \text{ mit } m_2 = \lfloor \frac{n}{p^2} \rfloor,$$

$$p^3, 2p^3, 3p^3, ..., m_3 p^3 \text{ mit } m_3 = \lfloor \frac{n}{p^3} \rfloor,$$

$$...$$

$$p^k, 2p^k, 3p^k, ..., m_k p^k \text{ mit } m_k = \lfloor \frac{n}{p^k} \rfloor$$

auf, denn:
Tritt $m_l \cdot p^l$, $1 \leq l \leq k$, unter den Zahlen $1, ..., n$ auf, muss $m_l \cdot p^l \leq n \Leftrightarrow m_l \leq \frac{n}{p^l}$ gelten, und ist $m_k \in \mathbb{N}_0$ maximal mit $m_k \cdot p^k \leq n \Leftrightarrow m_k \leq \frac{n}{p^k}$, so gilt nach der Definition der unteren Gauss-Klammer $m_k = \max\{z \in \mathbb{Z}; z \leq \frac{n}{p^k}\} = \lfloor \frac{n}{p^k} \rfloor$.
Nun gilt $\nu_p(n!) = \sum\limits_{k \geq 1} m_k = \sum\limits_{k \geq 1} \lfloor \frac{n}{p^k} \rfloor$.
Außerdem gilt: $n, p \in \mathbb{N} \Rightarrow \frac{n}{p^k} \geq 0$ und damit

$$\lfloor \frac{n}{p^k} \rfloor = 0 \ \Leftrightarrow \ \frac{n}{p^k} < 1 \ \Leftrightarrow \ p^k > n \ \Leftrightarrow \ k > \frac{\ln(n)}{\ln(p)}.$$

Somit ist die Summe endlich und es gilt:

$$\nu_p(n!) = \sum_{k \geq 1} \lfloor \frac{n}{p^k} \rfloor = \sum_{k=1}^{\lfloor \frac{\ln(n)}{\ln(p)} \rfloor} \lfloor \frac{n}{p^k} \rfloor.$$

b) Nach (1.3) gilt für $m, n \in \mathbb{N}$

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

mit geeigneten $\nu_p(m), \nu_p(n) \in \mathbb{N}_0$, $\nu_p(m) = 0, \nu_p(n) = 0$ für fast alle p.
Somit gilt

$$\nu_p(m \cdot n) = \nu_p(m) + \nu_p(n). \tag{4}$$

Behandeln wir zunächst die Fälle $j = 0$ und $j = n$. Es gilt

$$\nu_p(\binom{n}{0}) = \nu_p(\binom{n}{n}) = \nu_p(1) = 0 \leq \frac{\ln(n)}{\ln(p)}$$

für alle $n \in \mathbb{N}$, $p \in \mathbb{P}$.
Sei nun $j \in \{1, ..., n-1\}$. Mit Teil a) gilt:

$$\begin{aligned} \nu_p(\binom{n}{j}) &= \nu_p(\frac{n!}{j! \cdot (n-j)!}) \\ &\overset{(4)}{=} \nu_p(n!) - \nu_p(j!) - \nu_p((n-j)!) \\ &\overset{\text{a)}}{=} \sum_{k=1}^{\lfloor \frac{\ln(n)}{\ln(p)} \rfloor} \left(\lfloor \frac{n}{p^k} \rfloor - \lfloor \frac{j}{p^k} \rfloor - \lfloor \frac{n-j}{p^k} \rfloor \right) \end{aligned} \tag{5}$$

Zwischenbehauptung: Für $x, y \in \mathbb{R}$ gilt $\lfloor x + y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor \leq 1$.
Beweis: Für $a \in \mathbb{R}$, $z \in \mathbb{Z}$ gilt

1. $a = \lfloor a \rfloor + r_a$ mit einem $0 \leq r_a < 1$,
2. $\lfloor a + z \rfloor = \max\{n \in \mathbb{Z}; n \leq a + z\} = \max\{n \in \mathbb{Z}; n \leq a\} + z = \lfloor a \rfloor + z$.

Seien nun $x, y \in \mathbb{R}$, $x = \lfloor x \rfloor + r_x$, $y = \lfloor y \rfloor + r_y$ mit $0 \leq r_x, r_y < 1$.
Dann gilt $0 \leq r_x + r_y < 2$.

1. Fall: $0 \leq r_x + r_y < 1$: Dann gilt $\lfloor r_x + r_y \rfloor = 0$ und somit

$$\begin{aligned} \lfloor x + y \rfloor &= \lfloor \lfloor x \rfloor + r_x + \lfloor y \rfloor + r_y \rfloor \\ &= \lfloor x \rfloor + \lfloor y \rfloor + \lfloor r_x + r_y \rfloor \\ &= \lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1 \end{aligned}$$

2. Fall: $1 \leq r_x + r_y < 2$: Dann gilt $\lfloor r_x + r_y \rfloor = 1$ und somit

$$\begin{aligned} \lfloor x + y \rfloor &= \lfloor \lfloor x \rfloor + r_x + \lfloor y \rfloor + r_y \rfloor \\ &= \lfloor x \rfloor + \lfloor y \rfloor + \lfloor r_x + r_y \rfloor \\ &= \lfloor x \rfloor + \lfloor y \rfloor + 1 \end{aligned}$$

Insgesamt gilt also die gewünschte Abschätzung:

$$\begin{aligned} & \lfloor x+y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1 \\ \Leftrightarrow \quad & \lfloor x+y \rfloor - \lfloor x \rfloor - \lfloor y \rfloor \leq 1 \end{aligned}$$

Setzt man nun $x := \frac{j}{p^k}$ und $y := \frac{n-j}{p^k}$ in diese Zwischenbehauptung ein und wendet dies auf Gleichung (5) an, ergibt sich:

$$\nu_p(\binom{n}{j}) \overset{(5)}{=} \sum_{k=1}^{\lfloor \frac{\ln(n)}{\ln(p)} \rfloor} \left(\lfloor \frac{n}{p^k} \rfloor - \lfloor \frac{j}{p^k} \rfloor - \lfloor \frac{n-j}{p^k} \rfloor \right) \leq \lfloor \frac{\ln(n)}{\ln(p)} \rfloor$$

c) Sei $j \in \{0, ..., n\}$. Mit Teilaussage b) folgt direkt:

$$p^{\nu_p(\binom{n}{j})} \overset{b)}{\leq} p^{\frac{\ln(n)}{\ln(p)}} = e^{\frac{\ln(n)}{\ln(p)} \cdot \ln(p)} = e^{\ln(n)} = n$$

d) Sei $j \in \{0, ..., n\}$, $p \in \mathbb{P}$. Dann gilt:

$$p > n \;\Rightarrow\; p \nmid n! \;\Rightarrow\; p \nmid \binom{n}{j} = \frac{n!}{j!(n-j)!}.$$

D.h., dass für jede Primzahl $p \in \mathbb{P}$, die einen Binomialkoeffizienen $\binom{n}{j}$, $j = 0, ..., n$, teilt, $p \leq n$ gilt.
Zusammen mit dem Fundamentalsatz der Arithmetik folgt daraus:

$$\binom{n}{j} \overset{(1.3)}{=} \prod_{p \in \mathbb{P}} p^{\nu_p(\binom{n}{j})} = \prod_{p \in \mathbb{P}, p \leq n} p^{\nu_p(\binom{n}{j})} \overset{c)}{\leq} \prod_{p \in \mathbb{P}, p \leq n} n = n^{|\{p \in \mathbb{P}, p \leq n\}|} = n^{\pi(n)}$$

e) Für $a, n \in \mathbb{N}, 1 \leq a \leq n$ gilt

$$\frac{n+a}{a} = 1 + \frac{n}{a} \geq 2$$

und somit

$$\begin{aligned} 2^n &= 2 \cdot ... \cdot 2 \leq \frac{(n+1)}{1} \cdot \frac{(n+2)}{2} \cdot ... \cdot \frac{(n+n)}{n} = \frac{(n+1) \cdot ... \cdot (2n)}{1 \cdot ... \cdot n} \cdot \frac{n!}{n!} \\ &= \frac{(2n)!}{(n!)^2} = \frac{(2n)!}{(n!)(2n-n)!} = \binom{2n}{n} < \binom{2n}{n} + \sum_{k=0}^{n-1} \binom{2n}{k} + \sum_{k=n+1}^{2n} \binom{2n}{k} \\ &= \sum_{k=0}^{2n} \binom{2n}{k} = \sum_{k=0}^{2n} \binom{2n}{k} 1^k 1^{2n-k} = (1+1)^{2n} = 4^n. \end{aligned}$$

□

Als direkte Folgerung notieren wir das

(1.9) Lemma
Für alle $n \in \mathbb{N}$, $n \geq 2$, gilt

$$\pi(2n) - \pi(n) < \ln(4)\frac{n}{\ln(n)}.$$

Beweis.
Es gilt

$$\begin{aligned}\pi(2n) - \pi(n) &= |\{p \in \mathbb{P}; p \leq 2n\}| - |\{p \in \mathbb{P}; p \leq n\}| \\ &= |\{p \in \mathbb{P}; p \leq 2n\} \setminus \{p \in \mathbb{P}; p \leq n\}| \\ &= |\{p \in \mathbb{P}; n < p \leq 2n\}|. \end{aligned} \tag{6}$$

Sei nun $p \in \mathbb{P}$ mit $n < p \leq 2n$. Dann gilt:

$$p | 2n! = 1 \cdot ... \cdot 2n \text{ und } p \nmid n! = 1 \cdot ... \cdot n$$

Wegen $p \nmid n!$ folgt auch $p \nmid (n!)^2$, denn

$$p \mid (n!)^2 = n! \cdot n! \overset{\text{Def.}\mathbb{P}}{\Rightarrow} p \mid n! \text{ (oder } p \mid n! \text{)}$$

Das heißt, dass jede dieser Primzahlen im Zähler, aber nicht im Nenner (und somit in der Primfaktorzerlegung) von $\binom{2n}{n} = \frac{(2n)!}{(n!)^2} \in \mathbb{N}$ auftaucht. Damit gilt

$$\prod_{\substack{p \in \mathbb{P}, \\ n < p \leq 2n}} p \leq \binom{2n}{n}$$

Zusammen mit (1.8) e) folgt dann:

$$n^{\pi(2n)-\pi(n)} \overset{(6)}{=} n^{|\{p \in \mathbb{P}\ ;\ n < p \leq 2n\}|} = \prod_{\substack{p \in \mathbb{P}, \\ n < p \leq 2n}} n < \prod_{\substack{p \in \mathbb{P}, \\ n < p \leq 2n}} p \leq \binom{2n}{n} \overset{(1.8)\text{ e)}}{<} 4^n$$

Logarithmieren ergibt:

$$\begin{aligned} & (\pi(2n) - \pi(n)) \cdot \ln(n) < \ln(4^n) = n \cdot \ln(4) \\ \Leftrightarrow \quad & \pi(2n) - \pi(n) < \ln(4) \cdot \frac{n}{\ln(n)}. \end{aligned}$$

□

Eine untere Abschätzung für $\pi(n)$ liefert das

(1.10) Lemma
Für alle $n \in \mathbb{N}$, $n \geq 3$ gilt
$$\pi(n) > \frac{2}{3}\frac{n}{\ln(n)}$$

Beweis.
Für $n \in \mathbb{N}$ gilt $\binom{n}{0} = \binom{n}{n} = 1$ und nach (1.8) d) gilt $\binom{n}{j} \leq n^{\pi(n)}$ für alle $0 \leq j \leq n$.
Damit ergibt sich:

$$\begin{aligned}
2^n = (1+1)^n &= \sum_{j=0}^{n} \binom{n}{j} 1^j 1^{n-j} = \sum_{j=0}^{n} \binom{n}{j} \\
&= \binom{n}{0} + \sum_{j=1}^{n-1} \binom{n}{j} + \binom{n}{n} \leq \binom{n}{0} + \sum_{j=1}^{n-1} \underbrace{n^{\pi(n)}}_{\substack{\text{unabh.}\\ \text{von j}}} + \binom{n}{n} \\
&= 1 + (n-1)\cdot n^{\pi(n)} + 1 = n \cdot n^{\pi(n)} + 2 - n^{\pi(n)}
\end{aligned}$$

Wegen $n \geq 3$, also $n > 2$ gilt

$$\begin{aligned}
n^{\pi(n)} > 2 \ &\Rightarrow 2 - n^{\pi(n)} < 0 \\
&\Rightarrow n \cdot n^{\pi(n)} + 2 - n^{\pi(n)} < n \cdot n^{\pi(n)}
\end{aligned}$$

Beide Ungleichungen zusammengefasst ergeben dann $2^n < n \cdot n^{\pi(n)}$.
Logarithmieren liefert

$$\begin{aligned}
\ln(2^n) = n \cdot \ln(2) &< \ln(n \cdot n^{\pi(n)}) \\
&= \ln(n) + \pi(n) \cdot \ln(n) = \ln(n) \cdot (1 + \pi(n)) \\
\Leftrightarrow \quad \pi(n) &> \ln(2) \cdot \frac{n}{\ln(n)} - 1.
\end{aligned}$$

Für $x > e$ gilt $\ln(x) > \ln(e) = 1$. Die Abbildung $f : x \mapsto \frac{x}{\ln(x)}$ ist somit auf $[e, \infty)$ streng monoton wachsend, da für die Ableitung der Funktion auf (e, ∞) stets $f'(x) = \frac{\ln(x)-1}{(\ln(x))^2} > 0$ gilt. Damit gilt für $n \in \mathbb{N}$, $n > 200$:

$$\begin{aligned}
&\frac{n}{\ln(n)} \geq \frac{201}{\ln(201)} \approx 37{,}90 > 37{,}76 \approx \frac{1}{\ln(2) - \frac{2}{3}} \\
\Leftrightarrow\ &\frac{\ln(n)}{n} \leq \ln(2) - \frac{2}{3} \\
\Leftrightarrow\ &\ln(2) - \frac{\ln(n)}{n} \geq \frac{2}{3} \\
\Leftrightarrow\ &\ln(2) \cdot \frac{n}{\ln(n)} - 1 \geq \frac{2}{3} \cdot \frac{n}{\ln(n)}
\end{aligned}$$

und somit die Behauptung

$$\pi(n) > \frac{2}{3} \cdot \frac{n}{\ln(n)}$$

für $n > 200$. Für $n \in \mathbb{N}, 3 \leq n \leq 200$ verifiziert man die Behauptung mit Hilfe der Primzahltabelle im Anhang. □

Eine obere Abschätzung liefert das

(1.11) Lemma
Für alle $n \in \mathbb{N}$, $n \geq 2$ gilt

$$\pi(n) < 2 \cdot \frac{n}{\ln(n)}$$

Beweis.
Für die Zahlen $n \leq 2^8 = 256$ zeigen wir die Aussage anhand der Primzahltabelle im Anhang. Sei im Folgenden $n > 2^8$. Für diese Zahlen verifizieren wir die Behauptung per Induktion nach n.

(IA) $n = 257$: Es gilt $\pi(257) = 55 < 92,63 \approx 2 \cdot \frac{257}{\ln(257)}$.

(IV) Für ein beliebiges aber festes $n \geq 257$ gelte

$$\pi(m) < 2 \cdot \frac{m}{\ln(m)} \text{ für alle } m < n.$$

(IS) $n - 1 \mapsto n$:
1. Fall: Sei zunächst $n = 2m$ gerade. Nach Lemma (1.9) gilt

$$\pi(2m) - \pi(m) < \ln(4) \cdot \frac{m}{\ln(m)} \Leftrightarrow \pi(2m) < \pi(m) + \ln(4) \cdot \frac{m}{\ln(m)} \tag{7}$$

und mit der Induktionsvoraussetzung folgt

$$\begin{aligned}
\pi(n) = \pi(2m) &\overset{(7)}{<} \pi(m) + \ln(4) \cdot \frac{m}{\ln(m)} \\
&\overset{(IV)}{<} 2 \cdot \frac{m}{\ln(m)} + \ln(4) \cdot \frac{m}{\ln(m)} = \frac{2m}{\ln(m)} + \ln(2^2) \cdot \frac{m}{\ln(m)} \\
&= \frac{2m}{\ln(m)} + 2 \cdot \ln(2) \cdot \frac{m}{\ln(m)} = \frac{2m}{\ln(2m) - \ln(2)} + \frac{2m\ln(2)}{\ln(2m) - \ln(2)} \\
&= \frac{n}{\ln(n) - \ln(2)} + \frac{n\ln(2)}{\ln(n) - \ln(2)} = (1 + \ln(2)) \cdot \frac{n}{\ln(n) - \ln(2)}
\end{aligned} \tag{8}$$

Außerdem gilt:

$$\begin{aligned} n \geq 2^8 \;&\Rightarrow\; \ln(n) \geq \ln(2^8) = 8\ln(2) \\ &\Rightarrow\; \frac{1}{8}\ln(n) \geq \ln(2) \\ &\Rightarrow\; \ln(n) - \frac{1}{8}\ln(n) = \frac{7}{8}\ln(n) \leq \ln(n) - \ln(2) \\ &\Rightarrow\; \frac{1}{\ln(n) - \ln(2)} \leq \frac{8}{7}\frac{1}{\ln(n)} \end{aligned} \tag{9}$$

Kombinieren der Gleichungen (8) und (9) ergibt:

$$\pi(n) < (1 + \ln(2)) \cdot \frac{8}{7}\frac{1}{\ln(n)}$$

Wegen $(1 + \ln(2)) \cdot \frac{8}{7} < 2$ folgt die Behauptung für n gerade.

2. Fall: Sei nun $n = 2m + 1$ ungerade. Wie im Beweis zu Lemma (1.10) bereits gezeigt, ist die Abbildung $x \mapsto \frac{x}{\ln(x)}$ streng monoton steigend für $x \geq e$. Mit dem bereits bewiesenen Teil folgt dann

$$\begin{aligned} \pi(n) &= \pi(2m + 1) \leq \pi(2m) + 1 \\ &\overset{\text{1. Fall}}{<} (1 + \ln(2)) \cdot \frac{8}{7} \cdot \frac{2m}{\ln(2m)} + 1 \\ &< (1 + \ln(2)) \cdot \frac{8}{7} \cdot \frac{n}{\ln(n)} + 1 \\ &= \left((1 + \ln(2)) \cdot \frac{8}{7} + \frac{\ln(n)}{n} \right) \cdot \frac{n}{\ln(n)} \end{aligned}$$

Da $x \mapsto \frac{\ln(x)}{x}$ für $x \geq e$ monoton fallend ist, ergibt sich weiter

$$\begin{aligned} (1 + \ln(2)) \cdot \frac{8}{7} + \frac{\ln(n)}{n} &\overset{n > 2^8}{\leq} (1 + \ln(2)) \cdot \frac{8}{7} + \frac{\ln(2^8)}{2^8} \\ &= (1 + \ln(2)) \cdot \frac{8}{7} + \frac{8 \cdot \ln(2)}{256} \\ &= \frac{8}{7} + \left(\frac{8}{7} + \frac{1}{32} \right) \ln(2) < 2 \end{aligned}$$

Damit folgt die Behauptung

$$\pi(n) < \frac{2n}{\ln(n)}.$$

□

Die gerade bewiesenen oberen und unteren Abschätzungen für $\pi(n)$ gehen auf Chebyshev (1821-1894) zurück. Zusammen liefern sie

$$\frac{2}{3} < \frac{\pi(n)}{\frac{n}{\ln(n)}} < 2.$$

Damit folgt das

(1.12) Korollar
Es gilt

$$\lim_{x\to\infty} \frac{\ln(\pi(x))}{\ln(x)} = 1$$

Beweis.
Sei $x > 0$. Dann ist klar: $\pi(x) = |\{p \in \mathbb{P}; p \le x\}| \le x$.
Also gilt für $x > 0$: $\frac{\ln(\pi(x))}{\ln(x)} \le \frac{\ln(x)}{\ln(x)} = 1$.
Außerdem gilt nach Lemma (1.10) für $n \in \mathbb{N}$, $n \ge 3$, die Abschätzung

$$\pi(n) > \frac{2}{3}\frac{n}{\ln(n)}$$

Damit ergibt sich

$$\begin{aligned}\frac{\ln(\pi(n))}{\ln(n)} \ge \frac{\ln(\frac{2}{3}\frac{n}{\ln(n)})}{\ln(n)} &= \frac{\ln(\frac{2}{3}) + \ln(n) - \ln(\ln(n))}{\ln(n)} \\ &= 1 + \frac{\ln(\frac{2}{3}) - \ln(\ln(n))}{\ln(n)}\end{aligned}$$

wobei

$$\lim_{n\to\infty} \frac{\ln(\frac{2}{3}) - \ln(\ln(n))}{\ln(n)} \overset{\text{L'Hospital}}{=} \lim_{n\to\infty} -\frac{\frac{1}{\ln(n)}\cdot\frac{1}{n}}{\frac{1}{n}} = \lim_{n\to\infty} -\frac{1}{\ln(n)} = 0$$

und somit

$$\lim_{n\to\infty} \left(1 + \frac{\ln(\frac{2}{3}) - \ln(\ln(n))}{\ln(n)}\right) = 1$$

Insgesamt:

$$\underbrace{1 + \frac{\ln(\frac{2}{3}) - \ln(\ln(n))}{\ln(n)}}_{\overset{n\to\infty}{\to} 1} \le \frac{\ln(\pi(n))}{\ln(n)} \le 1$$

Mit dem Sandwich-Lemma folgt die Behauptung. □

Eine Umformung unsere elementarer Aussagen liefert auch eine Abschätzung für die n-te Primzahl p_n.

(1.13) Korollar
Ist $n \geq 2$, so gilt für die n-te Primzahl p_n die Abschätzung

$$\frac{1}{2}n\ln(n) < p_n < 3n\ln(n).$$

Beweis.
Ist $n \in \mathbb{N}$, $n \geq 2$, so gilt $p_n \geq 3$ und $\pi(p_n) = n$. Aus Lemma (1.11) folgt

$$n = \pi(p_n) < 2 \cdot \frac{p_n}{\ln(p_n)} \quad \Leftrightarrow \quad p_n > \frac{n\ln(p_n)}{2} \overset{p_n \geq n}{\geq} \frac{n\ln(n)}{2}$$

Anderseits gilt

$$n = \pi(p_n) \overset{(1.10)}{>} \frac{2}{3}\frac{p_n}{\ln(p_n)} \;\Leftrightarrow\; p_n < \frac{3}{2}n\ln(p_n) \tag{10}$$

Für $n \geq 9$ gilt $p_n \geq p_9 = 23$. Für $x \geq 23$ ist $x \mapsto \frac{\ln(x)}{\sqrt{x}}$ monoton fallend (da $\left(\frac{\ln(x)}{\sqrt{x}}\right)' = \frac{1-\ln(x)}{2\sqrt{x^3}} < 0$ für $x \geq 23$) und somit gilt $\frac{\ln(p_n)}{\sqrt{p_n}} \leq \frac{\ln(23)}{\sqrt{23}} \leq \frac{2}{3}$, also $\ln(p_n) \leq \frac{2}{3}\sqrt{p_n}$ für $n \geq 9$.

Eingesetzt in Ungleichung (10) ergibt sich für $n \geq 9$

$$\begin{aligned} & p_n < n\sqrt{p_n} && \Rightarrow\; p_n^2 < n^2 p_n \\ \Rightarrow\; & p_n < n^2 && \Rightarrow\; \ln(p_n) < \ln(n^2) = 2\ln(n). \end{aligned}$$

Setzt man diese Ungleichung wiederum in (10) ein, ergibt das die Behauptung für $n \geq 9$. Für $2 \leq n \leq 8$ nutzt man die Primzahltabelle im Anhang. $\square$

Man kann diese grobe Abschätzung noch verwenden, um die langsame Divergenz der unendlichen Reihe $\sum\limits_{k=1}^{\infty} \frac{1}{p_k}$ in (1.6) nachzuweisen.

Dazu zunächst eine Vorbemerkung:
Seien $p, q \in \mathbb{Z}$ mit $p < q$ und $f : [p,q] \to [0,\infty)$ eine monoton fallende Funktion. Dann gilt auf jedem Intervall $[n, n+1]$ für ein $n \in \mathbb{N}$ (mit $p \leq n, n+1 \leq q$)

$$f(n+1) \leq f(x) \leq f(n).$$

Daraus folgt für das Integral

$$\int_p^q f(x)dx \overset{p,q\in\mathbb{Z}}{=} \int_p^{p+1} f(x)dx + \int_{p+1}^{p+2} f(x)dx + \dots + \int_{q-1}^{q} f(x)dx$$

einmal die folgende Abschätzung nach oben

$$\int_p^q f(x)dx \leq f(p) + f(p+1) + \dots + f(q-1) = \sum_{k=p}^{q-1} f(k) \left(\leq \sum_{k=p}^{q} f(k) \right) \tag{11}$$

und andererseits die Abschätzung nach unten

$$\int_p^q f(x)dx \geq f(p+1) + f(p+2) + \dots + f(q) = \sum_{k=p+1}^{q} f(k). \tag{12}$$

Nun zur langsamen Divergenz der Reihe $\sum\limits_{k=1}^{\infty} \frac{1}{p_k}$:
Einerseits gilt

$$\begin{aligned}\sum_{n=1}^{N} \frac{1}{p_n} &= \frac{1}{2} + \sum_{n=2}^{N} \frac{1}{p_n} \geq \sum_{n=2}^{N} \frac{1}{p_n} \overset{(1.13)}{\geq} \frac{1}{3} \sum_{n=2}^{N} \frac{1}{n\ln(n)} \overset{(11)}{\geq} \frac{1}{3} \int_2^N \frac{1}{x\ln(x)}dx \\ &= \frac{1}{3} \ln(\ln(x))|_2^N = \frac{1}{3}(\ln(\ln(N)) - \ln(\ln(2))) \geq \frac{1}{3}\ln(\ln(N)).\end{aligned}$$

Andererseits:

$$\begin{aligned}\sum_{n=1}^{N} \frac{1}{p_n} &= \frac{1}{2} + \frac{1}{3} + \sum_{n=3}^{N} \frac{1}{p_n} \overset{(1.13)}{\leq} \frac{1}{2} + \frac{1}{3} + 2\sum_{n=3}^{N} \frac{1}{n\ln(n)} \\ &\overset{(12)}{\leq} \frac{1}{2} + \frac{1}{3} + 2\int_{n=2}^{N} \frac{1}{x\ln(x)}dx = \frac{5}{6} + 2(\ln(\ln(N)) - \ln(\ln(2))).\end{aligned}$$

Dabei ist $\ln(\ln(x))$ ist die Stammfunktion von $x \mapsto \frac{1}{x\ln(x)}$. D.h. die Reihe $\sum\limits_{n=1}^{N} \frac{1}{p_n}$ ist eingeschachtelt durch die zwei Funktionen $\frac{1}{3}\ln(\ln(N))$ und
$\frac{5}{6} + 2(\ln(\ln(N)) - \ln(\ln(2)))$, die beide sehr langsam gegen ∞ divergieren.

Für $N \geq 2$ gilt

$$\frac{1}{3} = \frac{\frac{1}{3}\ln(\ln(N))}{\ln(\ln(N))} \leq \frac{1}{N\ln(N)} \sum_{n=1}^{N} \frac{1}{p_n} \leq \frac{\frac{5}{6} + 2(\ln(\ln(N)) - \ln(\ln(2)))}{\ln(\ln(N))}$$

und somit ist die Folge

$$\left(\frac{1}{\ln(\ln(N))}\sum_{n=1}^{N}\frac{1}{p_n}\right)_{N\geq 2}$$

beschränkt, da

$$\lim_{n\to\infty}\frac{\frac{5}{6}+2(\ln(\ln(N))-\ln(\ln(2))}{\ln(\ln(N))}=\lim_{n\to\infty}2+\frac{\frac{5}{6}-2\ln(\ln(2))}{\ln(\ln(N))}=2$$

Mit Korollar (1.13) kann man auch noch folgendes zeigen:

(1.14) Korollar
Die Reihe

$$\sum_{p\in\mathbb{P}}\frac{1}{p\cdot\ln(p)}$$

konvergiert.

Beweis.
Nach Korollar (1.13) gilt für $n\in\mathbb{N}, n\geq 2$ die Abschätzung $p_n>\frac{1}{2}n\ln(n)$.
Damit folgt

$$\begin{aligned}\sum_{p\in\mathbb{P}}\frac{1}{p\cdot\ln(p)}&=\sum_{n=1}^{\infty}\frac{1}{p_n\cdot\ln(p_n)}=\frac{1}{2\cdot\ln(2)}+\sum_{n=2}^{\infty}\frac{1}{p_n\cdot\ln(p_n)}\\&<\frac{1}{2\cdot\ln(2)}+\sum_{n=2}^{\infty}\frac{1}{\frac{1}{2}n\ln(n)\cdot\ln(\frac{1}{2}n\ln(n))}\end{aligned}$$

Für $n\geq 8$ gilt $\ln(n)\geq 2$ und sowie $\frac{1}{2}n\ln(n)\geq n$ als auch $\ln(\frac{1}{2}n\ln(n))\geq\ln(n)$.
Also folgt

$$\sum_{n=8}^{\infty}\frac{1}{\frac{1}{2}n\ln(n)\cdot\ln(\frac{1}{2}n\ln(n))}\leq\sum_{n=8}^{\infty}\frac{1}{\frac{1}{2}n(\ln(n))^2}=2\sum_{n=8}^{\infty}\frac{1}{n(\ln(n))^2}$$

Wir wollen nun das Integralvergleichskriterium anwenden, das besagt:
Ist $p\in\mathbb{Z}$, $f:[p,\infty)\to[0,\infty)$ eine monoton fallende Funktion, dann gilt:

$$\sum_{n=p}^{\infty}f(n)\text{ konvergiert }\Leftrightarrow\int_{p}^{\infty}f(x)dx\text{ ex.}$$

Wir wählen in unserem Fall $p=8$ und $f(x):=\frac{1}{x(\ln(x))^2}$. Dann gilt
$f'(x)=-\frac{(\ln(x))^2+2\ln(x)}{x^2(\ln(x))^4}<0$ für $x\geq 8$. Also ist f auf $[8,\infty)$ monoton fallend.

Außerdem ist $f(x) \geq 0$ für alle $x \in [8, \infty)$. Die Voraussetzungen für das Integralvergleichskriterium sind also erfüllt. Zu zeigen bleibt also

$$\int_8^\infty \frac{1}{x(\ln(x))^2} dx < \infty.$$

Dazu:

$$\int_8^\infty \frac{1}{x(\ln(x))^2} dx = -\frac{1}{\ln(x)}\Big|_8^\infty = -\underbrace{\lim_{x\to\infty} \frac{1}{\ln(x)}}_{=0} + \frac{1}{\ln(8)} = \frac{1}{\ln(8)} < \infty$$

□

(1.15) Korollar
Für jedes $n \in \mathbb{N}$ liegt im Intervall $(n, 4n]$ mindestens eine Primzahl und es gilt

$$\lim_{n\to\infty} |(\mathbb{P} \cap (n, 4n])| = \infty.$$

Beweis.
Es gilt

$$\begin{aligned}
|(\mathbb{P} \cap (n, 4n]))| &= |\{p \in \mathbb{P}; n < p \leq 4n\}| \\
&= |\{p \in \mathbb{P}; p \leq 4n\} \setminus \{p \in \mathbb{P}; p \leq n\}| \\
&= \pi(4n) - \pi(n) \\
&\overset{(1.10}{\underset{(1.11)}{>}} \frac{2}{3}\frac{4n}{\ln(4n)} - 2\frac{n}{\ln(n)} = \frac{n}{\ln(n)}\left(\frac{8}{3}\frac{\ln(n)}{\ln(n)+\ln(4)} - 2\right) \qquad (13)
\end{aligned}$$

Für $1 \leq n \leq 64$ verifiziert man mit der Primzahltabelle im Anhang, dass $|(\mathbb{P} \cap (n, 4n]))| > 0$ gilt.
Für $n > 64$ nutzen wir die Ungleichungen $\frac{n}{\ln(n)} > \frac{64}{\ln(64)} > 0$ und $\frac{8}{3}\frac{\ln(n)}{\ln(n)+\ln(4)} - 2 > 0$.
Die zweite Ungleichung erhält man durch

$$\begin{aligned}
n > 64 &\Rightarrow \ln(n) > \ln(64) = \ln(4^3) = 3\ln(4) \\
&\Rightarrow 8\ln(n) > 6\ln(n) + 6\ln(4) \\
&\Rightarrow \frac{8}{3}\frac{\ln(n)}{\ln(n)+\ln(4)} > 2.
\end{aligned}$$

Also ist $|(\mathbb{P} \cap (n, 4n])| > 0$ für alle $n \in \mathbb{N}$ gezeigt.

Bleibt noch $\lim\limits_{n\to\infty} |(\mathbb{P} \cap (n, 4n])| = \infty$ zu zeigen. Betrachte dazu

$$\begin{aligned}
\frac{8}{3}\frac{\ln(n)}{\ln(n)+\ln(4)} - 2 - \frac{2}{3} &= \frac{8}{3}\frac{\ln(n)}{\ln(n)+\ln(4)} - \frac{8}{3} \\
&= \frac{8}{3}\left(\frac{\ln(n)}{\ln(n)+\ln(4)} - 1\right) \\
&= -\frac{8}{3}\frac{\ln(4)}{\ln(n)+\ln(4)} \underset{n\to\infty}{\to} 0 \\
\Rightarrow \quad \lim_{n\to\infty} \frac{8}{3}\frac{\ln(n)}{\ln(n)+\ln(4)} - 2 = \frac{2}{3}
\end{aligned}$$

Weiter gilt

$$\lim_{n\to\infty} \frac{n}{\ln(n)} = \lim_{n\to\infty} \frac{1}{\frac{1}{n}} = \lim_{n\to\infty} n = \infty$$

Zusammen:

$$\lim_{n\to\infty} |(\mathbb{P} \cap (n, 4n]))| \overset{(13)}{=} \lim_{n\to\infty} \frac{n}{\ln(n)} \left(\frac{8}{3}\frac{\ln(n)}{\ln(n)+\ln(4)} - 2\right) = \infty.$$

□

Mit etwas mehr Aufwand kann man sogar das BERTRANDsche Postulat

$$|(\mathbb{P} \cap (n, 2n]))| > 0 \text{ für alle } n \in \mathbb{N}$$

zeigen.

Das nächste Lemma macht deutlich, dass der Abstand zwischen zwei aufeinanderfolgenden Primzahlen beliebig groß werden kann:

(1.16) Lemma
Zu jedem $n \in \mathbb{N}$ gibt es n aufeinanderfolgende natürliche Zahlen, die keine Primzahlen sind.

Beweis.
Wir zeigen die Aussage durch einen Konstruktionsbeweis.
Sei $a_j := (n+1)! + j$ für $j = 2, ..., n+1$. Dann sind die a_j n aufeinanderfolgende natürliche Zahlen. Es gilt $j \leq n+1 \Rightarrow j \mid (n+1)!$ und natürlich $j \mid j$. Somit gilt $j \mid a_j$ für alle $j = 2, ..., n+1$. Wegen $n \in \mathbb{N}$, also $n > 0$, gilt $a_j > j$. D.h. j ist ein echter Teiler von a_j und somit gilt $a_j \notin \mathbb{P}$ für $j = 2, ..., n+1$. Somit sind die a_j n aufeinanderfolgende natürliche Zahlen, die keine Primzahlen sind. □

Anders ausgedrückt besagt (1.16)

$$\sup\{p_{n+1} - p_n; n \in \mathbb{N}\} = \infty$$

§3 Anhang

Primzahltabelle

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499 503 509 521 523 541 547 557 563 569 571 577 587 593 599 601 607 613 617 619 631 641 643 647 653 659 661 673 677 683 691 701 709 719 727 733 739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 857 859 863 877 881 883 887 907 911 919 929 937 941 947 953 967 971 977 983 991 997 1009 ...