Die Dichte der Primzahlen

Bachelorarbeit

vorgelegt am: 12.10.2018

am Fachbereich Mathematik der Johannes Gutenberg-Universität Mainz

Name:	Patrick Abels
Matrikelnummer:	2723370
Universität:	Johannes Gutenberg-Universität Mainz
Fachbereich:	08
Studiengang:	Mathematik und Informatik
Studienjahrgang:	2015
Erstgutachter:	Dr. Cynthia Hog-Angeloni, Akad. Rat
Zweitgutachter:	Dr. Anton Malevich

Inhaltsverzeichnis

Kapitel 1

Einleitung

Bereits im antiken Griechenland waren die Primzahlen ein Anlass großer Faszination. Ausschlaggebend für Bereiche der Kunst oder Biologie waren Fragen, die teilweise bis heute nicht endgültig geklärt sind. Unter Anderem interessiert man sich früh für mögliche Abschätzungen der Anzahl $\pi(x)$ von Primzahlen kleiner oder gleich einer Zahl x. Seither werden entsprechende Näherungen immer besser, beginnend bei $\log(\log(x))$ bis hin zu $\frac{x}{\log(x)}$. Diese Arbeit arbeitet darauf hin, drei bedeutsame Abschätzungen für $\pi(x)$ zu beweisen: $\log(\log(x))$, $\frac{\log(x)}{2\log(2)}$ und $\frac{x}{\log(x)}$.

Bezüglich des asymptotischen Verhaltens der Funktionen $\frac{x}{\log(x)}$ und $\pi(x)$ lassen sich zwei grundlegende Aussagen treffen, welche klar voneinander abzugrenzen sind:

Zunächst lässt sich die erste Aussage zeigen, dass

$$f \sim g \; bzw. \; \frac{\pi(x)}{\frac{x}{\log(x)}} \longrightarrow 1$$

gilt, die beiden Funktionen sind also asymptotisch gleich.

Die zweite Aussage, welche Hauptbestandteil dieser Arbeit ist, wurde 1852 von Tschebyscheff bewiesen. Sie besagt für alle $n \in \mathbb{N}$ mit $n \geq 4$, dass

$$\frac{n}{\log(n)} \asymp \pi(n) \; bzw. \; \frac{1}{4}\frac{n}{\log(n)} \leq \pi(n) \leq 6\frac{n}{\log(n)}$$

gilt.

Dafür lernen wir in Kapitel 2 grundlegende Begriffe zum Verständnis nachfolgender Sachverhalte kennen. Mit Hinblick auf die Näherungen werden wir Primzahlen als solche und insbesondere den Fundamentalsatz der Zahlentheorie, der sich mit der Unendlichkeit der Primzahlmenge beschäftigt, verstehen. Dazu lernen wir in Kapitel 3 neue Zahlenfolgen kennen und nutzen ihre Eigenschaften für den Beweis. Mit Definitionen, Notationen, Beispielen und dem Fundamentalsatz der Zahlentheorie im Koffer befassen wir uns in Kapitel 4 mit dem eigentlichen Thema der Arbeit: Abschätzungen der Menge der Primzahlen bis zu einer natürlichen Zahl x. Die entsprechenden Beweise sind teilweise erklärt, teilweise sprengt das nötige Hintergrundwissen jedoch den Rahmen dieser Arbeit, sodass manche Schritte in all ihrer Brillianz hinzunehmen und als Inspiration aufzufassen sind.

Kapitel 2

Grundlagen

Zum besseren Verständnis der Arbeit werden grundlegende Symbole sowie gängige Konventionen vorab geklärt.

2.1 Notationen

Seien f und g reellwertige Funktionen abhängig von x.

$$f = O(g) \iff \exists A \; mit \; |f| < Ag$$

$$f = o(g) \iff \frac{f}{g} \xrightarrow[x \to \infty]{} 0$$

$$f \sim g \iff \frac{f}{g} \xrightarrow[x \to \infty]{} 1$$

$$f \asymp g \iff \exists A, B \; mit \; Ag < f < Bg$$

Bemerkung:

$f \sim g \iff f = g{+}o(g) \iff f = g(1{+}o(1)) \Longrightarrow$ f und g sind asymptotisch gleich.[1, S. 7]

2.2 Mengen

Im Folgenden bezeichnen ...,-3,-2,-1,0,1,... ganze Zahlen $\mathbb{Z}$, 0,1,... Nicht-negative ganze Zahlen $\mathbb{N}_0$ und 1,2,... Positive Zahlen $\mathbb{N}$. Buchstaben wie a,b,A,B,... ersetzen Zahlen, genauer Konstanten. Der Buchstabe p ersetzt, wenn nicht anders angegeben, eine Primzahl. [1, S. 1]

2.3 Division mit Rest

Satz 1. *$\forall$ a, b aus $\mathbb{Z}$ $\exists!$ q, r, sodass $a = bq + r$ mit $0 \leq r < b$.*

Beweis.
Existenz:
Ohne Einschränkung gilt b>0. Die Menge $\{w \in \mathbb{Z} : bw > a\}$ ist somit nicht leer und hat ein kleinstes Element w. Setze $q = w - 1$ und $r = a - qb$. Da für w gilt, dass $bw > a$ und q gerade $w - 1$ ist, erhalten wir $r = a - qb = a - (w-1)b = a - wb + b$. Wir wollen zeigen, dass dieser Term kleiner b ist, also $a - wb + b < b$. Subtrahieren wir auf beiden Seiten b und bringen wb auf die rechte Seite, erhalten wir die wahre Aussage $a < wb$. Da w das kleinste Element mit $bw > a$ ist, gilt für q gerade $qb \leq a$ und somit $r = a - qb \geq 0$.
Eindeutigkeit:
$bq_1 + r_1 = a = bq_2 + r_2$, ohne Einschränkung $r_2 \leq r_1$. Dann $0 \leq r_1 - r_2 = b(q_2 - q_1) < |b|$, also $q_1 = q_2$ und $r_1 = r_2$. [3, S. 8] □

2.4 Teilbarkeit, Teilerfremdheit

Definition 1. *Wir nennen $a \in \mathbb{Z}$ teilbar duch $b \in \mathbb{Z}$ $\Leftrightarrow$ $\exists$ $c \in \mathbb{Z}$ mit $a = bc$ und schreiben $b|a$.* [*3*, S. 9]

Bemerkung: 1|a $\forall$a, a|a $\forall$a, a|0 $\forall$a.

Definition 2. *Wir nennen a und b teilerfremd $\Leftrightarrow$ $\forall$ $t \in \mathbb{N}$ gilt: aus $t|a$ und $t|b$ folgt $t = 1$.* [*3*, S. 9]

2.5 Primalität

Definition 3. *Wir nennen $p \in \mathbb{N}$ prim $\Leftrightarrow$ $p > 1$ und p hat keine positiven Teiler außer 1 und p.*

Bemerkung: p ist äquivalent dazu prim, genau dann wenn aus $p > 1$ und $p = ab$ folgt $a = 1$ oder $b = 1$. Sonst nennen wir p zusammengesetzt. [1, S. 2]

2.6 Fundamentalsatz der Arithmetik

Satz 2. *Jedes $n \in \mathbb{N} \backslash \{1\}$ hat eine eindeutige Darstellung $n = p_1^{r_1} * p_2^{r_2} * ... * p_s^{r_s}$, genannt Primfaktorzerlegung.* [*1*, S. 2]

Beweis.
Existenz:
2 ist klar prim. Angenommen $n > 2$ ist nicht prim, dann existieren nach Definition a und b mit $n = ab$ mit $a, b \neq 1$. Da $a, b < n$, zerlege beide wiederum in ihre Primfaktoren und sortiere diese. Induktiv wird somit klar, dass auch n in Primfaktoren zerlegbar ist und eine Darstellung der Form

$$n = p_1^{r_1} * p_2^{r_2} * ... * p_s^{r_s}$$

entsteht.

Eindeutigkeit:
Eindeutige Zerlegung der 2 ist klar (Induktionsvoraussetzung). Sei also $n > 2$ mit

$$n = p_1^{r_1} * p_2^{r_2} * ... * p_s^{r_s} = q_1^{k_1} * q_2^{k_2} * ... * q_t^{k_t},$$

ohne Einschränkung $p_1 < q_1$. Es folgt, dass ohne Beachtung der Exponenten

$$n > p_1(p_2 * ... * p_s - q_2 * ... * q_t) = (q_1 - p_1) * q_2 * ... * q_t \geq 2,$$

also ist

$$p_1(p_2 * ... * p_s - q_2 * ... * q_t) = (q_1 - p_1) * q_2 * ... * q_t$$

nach Induktionsvoraussetzung eindeutig. Wegen $p_1 < q_1 < q_i$ ist folglich p_1 kein Teiler von $q_1 - p_1$ also Primfaktor von $p_1(p_2 * ... * p_s - q_2 * ... * q_t)$, jedoch kein Primfaktor von$(q_1 - p_1) * q_2 * ... * q_t$. Dies ist ein Widerspruch. [3, S. 10] □

Kapitel 3

Die Unendlichkeit der Primzahlen - Der Zweite Satz von Euklid

Satz 3. *Es existieren unendlich viele Primzahlen.* [*3*, S. 11]

Dieser Satz wird nachfolgend auf verschiedenen Wegen bewiesen. Dazu muss zunächst etwas Vorarbeit geleistet werden: Wir führen Fermat-Zahlen und Mersenne-Zahlen ein, beweisen die Divergenz der unendlichen Reihe über die Kehrwerte der Primzahlen und geben einen kurzen Einstieg in die Topologie.

Allen Beweisen ist gemein, dass ursprünglich von der Endlichkeit der Primzahlmenge ausgegangen wird. Diese Annahme wird auf verschiedenen Wegen zum Widerspruch geführt.

3.1 Fermat- und Mersenne-Zahlen

Definition 4. *Die n-te Fermat-Zahl ist gegeben durch: $F_n := 2^{2^n} + 1$.* [*1*, S. 14]

Bemerkung: Die Fermat-Zahlen sind mindestens für $n = 0, 1, 2, 3, 4$ prim.

Definition 5. *Die p-te Mersenne-Zahl mit p prim ist gegeben durch: $M_p := 2^p - 1$.* [*1*, S. 16]

Bemerkung: Die Mersenne-Zahlen sind unter Anderem für $p = 2, 3, 5, 7,$
$13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213$
prim. [1, S. 16]

Satz 4. $\sum_{p\ prim} \frac{1}{p}$ *divergiert.*

Beweis. (1)
Angenommen, die Reihe $\sum_{\text{p prim}} \frac{1}{p}$ konvergiert. Wähle j, sodass der Rest nach den ersten j Termen kleiner $\frac{1}{2}$ ist, also

$$\frac{1}{p_{j+1}} + \frac{1}{p_{j+2}} + ... < \frac{1}{2}.$$

Die Anzahl $n \leq x$ der durch p teilbaren Zahlen ist mindestens $\frac{x}{p}.x - N(x)$, die Anzahl an $n \leq x$ der durch ein oder mehrere p_{j+1} teilbaren Zahlen, ist höchstens $\frac{x}{p_{j+1}} + \frac{x}{p_{j+2}} + ... < \frac{x}{2}$. Wegen

$$N(x) \leq 2^j \sqrt{x}$$

folgt

$$\frac{x}{2} < N(x) \leq 2^{j\sqrt{x}}$$

für $x < 2^{2j+2}$, was für $x \geq 2^{2j+2}$ falsch ist. [1, S. 17] $\square$

Beweis. (2)
Angenommen $\sum_{\text{p prim}} \frac{1}{p}$ konvergiert, dann existiert ein $k \in \mathbb{N}$ mit

$$\sum_{i \geq k+1} \frac{1}{p_i} < \frac{1}{2}.$$

Für alle $N \in \mathbb{N}$ gilt:

$$\sum_{i \geq k+1} \frac{N}{p_i} < \frac{N}{2}. \qquad (*)$$

Seien nun N_b und N_s definiert durch:

$$N_b := \#\{n \leq N | \text{n ist teilbar durch mindestens ein } p \in \{p_{k+1}, ...\}\}$$

und

$$N_s := \#\{n \leq N | \text{n ist ausschließlich teilbar durch } p \in \{p_1, ..., p_k\}\}.$$

Wir bemerken außerdem, dass

$$\lfloor \frac{N}{p_i} \rfloor = \#\{n \leq N | \text{n ist Vielfaches von } p_i\}.$$

Nun gilt wegen $(*)$:

$$N_b \leq \sum_{i \geq k+1} \lfloor \frac{N}{p_i} \rfloor < \frac{N}{2}. \qquad (**)$$

Schreiben wir jedes n der Form $n = a_n {b_n}^2$, mit a_n als den quadratfreien Teil, erkennen wir, dass es genau 2^k verschiedene quadratfreie Teile gibt. Wegen

$$b_n \leq \sqrt{n} \leq \sqrt{N}$$

sehen wir, dass es höchstens $\sqrt{N}$ verschiedene Quadratteile gibt, und es folgt

$$N_s \leq 2^k \sqrt{N}.$$

Zumal (∗∗) für alle N gilt, suche N mit $2^k\sqrt{N} \leq \frac{N}{2} \Leftrightarrow N = 2^{2k+2}$. [2, S. 6] □

Definition 6. *Eine Topologie auf einer Menge X ist eine Menge T von Teilmengen von X, so dass die folgenden Axiome gelten:*
1. Die Teilmengen $\emptyset$ und X sind offen.
2. Der Durchschnitt endlich vieler offener Mengen ist offen.
3. Die Vereinigung beliebig vieler offener Mengen ist offen. [4, S. 7]

3.2 Euklids Beweis

Angenommen die Menge P der Primzahlen sei endlich mit $P = \{p_1, p_2, ..., p_r\}$. Setze nun $N := p_1 * p_2 * ... * p_r + 1$. Trivialerweise ist $N - 1$ teilbar durch jedes der p_i. Daher kann kein p_i auch N teilen. Nach dem Fundamentalsatz der Arithmetik muss jedoch auch N eindeutig durch Produkt von Primzahlen darstellbar sein. P kann also nicht endlich sein. [2, S. 3] □

3.3 Goldbachs Beweis

Dieser Beweis fußt auf den Fermat-Zahlen. Wegen $\prod_{k=0}^{n-1} F_k = F_n - 2$ (Beweis folgt) gilt für je zwei Fermat-Zahlen F_k und F_n, dass kein $p \neq 2$ exisiert, welches F_k und F_n teilt. Wäre die Menge der Primzahlen endlich, wäre auch die Menge der Fermat-Zahlen endlich, was falsch ist.
Wir beweisen obige Aussage induktiv nach n: Für $n = 1$ haben wir $F_0 = 3$ und $F_1 - 2 = 3$. Induktiv erhalten wir

$$\begin{aligned}\prod_{k=0}^{n} F_k = \left(\prod_{k=0}^{n-1} F_k\right) * F_n = (F_n - 2) * F_n = (2^{2^n} - 1)(2^{2^n} + 1) \\ = 2^{2^{n+1}} - 1 = F_{n+1} - 2.\end{aligned}$$

[2, S. 3,4] □

3.4 Beweis (Autor unbekannt)

Dieser Beweis fußt auf den Mersenne-Zahlen. Sei nun q ein Primteiler von $2^p - 1$, sodass $2^p \equiv 1 \ (mod\ q)$. Da p prim, hat die 2 in der Gruppe $\mathbb{Z}_q \backslash \{0\}$ die Ordnung p. Diese Gruppe enthält $q - 1$ Elemente. Nach dem Satz von Lagrange teilt die Ordnung jedes Elements einer Gruppe die Gruppengröße, sodass $p|q - 1$ und daher $p < q$.
Für jedes p sind daher alle Primteiler q von M_p größer als p, was im Widerspruch zur Endlichkeit der Primzahlmenge steht. [2, S. 4] □

3.5 Eulers Beweis

Für $n \leq x \leq n + 1$ gilt:

$$\begin{aligned}\log(x) \leq 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{n-1} + \frac{1}{n} \leq & \sum_{m \in \mathbb{N} \text{ enthält nur Primfaktoren } p \leq x} \frac{1}{m} \\ &= \prod_{p \in P \wedge p \leq x} \sum_{k \geq 0} \frac{1}{p^k} = \prod \frac{1}{1 - \frac{1}{p}} \\ &= \prod \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1} \leq \prod \frac{k+1}{k} = \pi(x) + 1.\end{aligned}$$

Die Gleichheit $\sum \frac{1}{m} = \prod \sum \frac{1}{p^k}$ gilt, da jedes m eindeutig als $\prod_{p \leq x} p^{k_p}$ geschrieben werden kann. Die nachfolgende Gleichheit folgt unmittelbar wegen der geometrischen Reihe mit Faktor $\frac{1}{p}$. Die letzte Ungleichung gilt, da $p_k \geq k + 1$. Wäre nun die Menge der Primzahlen beschränkt, wäre auch der Logarithmus beschränkt, was ein Widerspruch ist. [2, S. 4,5] □

3.6 Fürstenbergs Beweis

Sei $N_{a,b} := \{a + nb | n \in \mathbb{Z}\}, a, b \in \mathbb{Z}, b > 0$ Topologie, für die gilt:

1. Jede nicht leere offene Menge ist unendlich;
2. Jede Menge $N_{a,b}$ ist abgeschlossen.

Jede Zahl hat mindestens einen Primteiler, sodass gilt: $\mathbb{Z} \backslash \{1, -1\} = \cup_{p \in P} N_{0,p}$, wobei P die Menge der Primzahlen ist. Wäre P endlich, wäre wegen 1. und 2. die Menge $\{1, -1\}$ offen, was nach 1. falsch ist. [2, S. 5] □

3.7 Erdös' Beweis

Wir berufen uns nun auf den Satz über die Divergenz der Reihe $\sum_{\text{p prim}} \frac{1}{p}$. Wäre nun die Primzahlmenge endlich, muss $\sum_{\text{p prim}} \frac{1}{p}$ konvergieren, was nach Satz 4 falsch ist. [2, S. 6] $\square$

Kapitel 4

Approximation von $\pi(x)$

Nachdem wir gesehen haben, dass die Menge der Primzahlen unendlich ist, interessiert uns, ob man die Zahl der Primzahlen bis zu einer Zahl x in irgendeiner Weise abschätzen kann.
Historisch gesehen fingen solche Abschätzungen bereits Hunderte von Jahren v. Chr. an und wurden bis heute immer exakter. Wir untersuchen im Folgenden genauer die Näherungen $\log(\log(x))$, $\frac{\log(x)}{2\log(2)}$ und $\frac{x}{\log(x)}$.
Wir bezeichnen die Menge der Primzahlen bis einschließlich x mit $\pi(x)$.

4.1 Logarithmusfunktion

Die Funktion $\log(x) := \int_1^x \frac{1}{t}dt$ ist die Umkehrfunktion von e^x. $\log(x)$ geht langsamer gegen unendlich als jede Potenz von x, $\log(\log(x))$ geht langsamer gegen unendlich als jede Potenz von $\log(x)$, und so weiter. [1, S. 9]

4.2 $\pi(x) \geq \log(\log(x)), x \geq 2$

Setze

$$q := 2 * ... * p + 1,$$

mit p als der n-ten Primzahl p_n. Klar gilt:

$$q < {p_n}^n + 1$$

und

$$p_{n+1} < {p_n}^n + 1$$

für $n > 1$. Angenommen

$$p_n < 2^{2^n} \qquad (*)$$

für $n = 1, ..., N$. Dann würde nach Euklid gelten:

$$p_{N+1} \leq p_1 * p_2 * ... * p_N + 1 < 2^{2+4+...+2^N} + 1 < 2^{2^{N+1}}.$$

Angenommen $n \geq 4$ und $e^{e^{n-1}} < x \leq e^{e^n}$, dann

$$e^{n-1} > 2^n,$$

$$e^{e^{n-1}} > 2^{2^n}$$

und somit

$$\pi(x) \geq \pi(e^{e^{n-1}}) \geq \pi(2^{2^n}) \geq n,$$

wegen $(*)$. Aufgrund von $\log(\log(x)) \leq n$ folgt

$$\pi(x) \geq \log(\log(x))$$

für $x > e^{e^3}$ und offensichtlich auch für $2 \leq x \leq e^{e^3}$. [1, S. 12] □

4.3 $\pi(x) \geq \frac{\log(x)}{2\log(2)}, x \geq 1$

Setze $j := \pi(x)$, sodass $p_{j+1} > x$ und $N(x) = x$. Es folgt $x = N(x) \leq 2^{\pi(x)}\sqrt{x}$, also $2^{\pi(x)} \geq \sqrt{x}$. Nehmen wir auf beiden Seiten den Logarithmus, folgt die Behauptung. [1, S. 17] □

4.4 Der Satz von Tschebyscheff

Satz 5. $\pi(x) \asymp \frac{x}{\log(x)}$.

Dieser Beweis ist sehr komplex, daher wird er unterteilt. Es werden die zwei Funktionen

$$\Psi(x) := \sum_{p^m \leq x} \log(p)$$

und

$$\Theta(x) := \sum_{p \leq x} \log(p) = \log\left(\prod_{p \leq x} p\right)$$

eingeführt und gezeigt, dass sie sich asymptotisch gleich verhalten. Beispiel: $\Psi(12) = 3\log(2) + 2\log(3) + \log(5) + \log(7) + \log(11)$ bzw. $\Theta(12) = \log(2) + \log(3) + \log(5) + \log(7) + \log(11)$. Nachdem danach gezeigt wird, dass sich beide Funktionen asymptotisch gleich wie x verhalten, wird mit dem Beweis abgeschlossen, dass $\pi(x)$ asymptotisch gleich zu $\Theta(x)$ verläuft, woraus mithilfe der ersten beiden Teilbeweise die Behauptung folgt. [6, S. 60]

4.4.1 $\Psi(x) = \Theta(x) + O(x^{\frac{1}{2}} \log^2(x))$

Für $U(x) := kgV\{k \in \mathbb{N} | k \leq x\}$ gilt:

$$\Psi(x) = \log(U(x)),$$

was klar wird, wenn wir folgendes Beispiel betrachten:

$$\begin{aligned}\Psi(12) = 3\log(2) + 2\log(3) + \log(5) + \log(7) + \log(11)\\ = \log(2*2*2*3*3*5*7*11) = \log(27720)\\ = \log(kgV(1,2,3,4,5,6,7,8,9,10,11,12)) = \log(U(12)).\end{aligned}$$

Außerdem können wir schreiben

$$\Psi(x) = \sum_{p \leq x} \lfloor \frac{\log(x)}{\log(p)} \rfloor * \log(p),$$

zumal im obigen Beispiel für $p = 2$ gerade $\lfloor \frac{\log(12)}{\log(2)} \rfloor = \lfloor \log_2(12) \rfloor = 3$ die Vielfachheit der 2 ist. Wegen

$$p^2 \leq x \Leftrightarrow p \leq x^{\frac{1}{2}}, p^3 \leq x \Leftrightarrow p \leq x^{\frac{1}{3}}, ...$$

folgt

$$\Psi(x) = \Theta(x) + \Theta(x^{\frac{1}{2}}) + ... = \sum_{x^{\frac{1}{m}} \geq 2 \Leftrightarrow m \leq \frac{\log(x)}{\log(2)}} \Theta(x^{\frac{1}{m}}).$$

Dabei sind $\Theta(x)$ die Logarithmen der Zahlen bis x aufaddiert, $\Theta(x^{\frac{1}{2}})$ die Logarithmen derer Zahlen mit Vielfachheit 2, und so weiter. Offensichtlich ist $\Theta(x) < x\log(x)$ für $x \geq 2$, also

$$\Theta(x^{\frac{1}{m}}) < x^{\frac{1}{m}} \log(x) \leq x^{\frac{1}{2}} \log(x)$$

für $m \geq 2$ und

$$\sum_{m \geq 2} \Theta(x^{\frac{1}{m}}) = O(x^{\frac{1}{2}} \log^2(x)),$$

weil in der Reihe nur $O(\log(x))$ Terme vorkommen. Somit folgt die Behauptung. [1, S. 340,341]

4.4.2 $\Psi(x) \asymp x$ und $\Theta(x) \asymp x$

Wir wollen zeigen, dass A,B,C und D existieren, sodass $Ax < \Theta(x) < Bx$ bzw. $Cx < \Psi(x) < Dx$ für $x \geq 2$. Nachdem bewiesen wurde, dass $\Psi(x) = \Theta(x) + O(x^{\frac{1}{2}} \log^2(x))$ gilt, haben wir bereits die Existenz der Konstanten A

und D bewiesen. Wir erinnern uns dazu an die Definition der O-Notation. Es reicht folglich zu zeigen, dass $\Psi(x) > Cx$ bzw. $\Theta(x) < Bx$. Genauer lässt sich induktiv sogar beweisen, dass

$$\Psi(x) \geq \frac{1}{4} x \log(2) \qquad (*)$$

und

$$\Theta(x) < 2x \log(2). \qquad (**)$$

Wir führen zunächst eine, wie bewiesen werden kann, ganze Zahl M ein:

$$M := \frac{(2m+1)!}{m!(m+1)!} = \frac{(2m+1)(2m)...(m+2)}{m!}.$$

Wir stellen fest, dass

$$2M < 2^{2m+1}$$

und

$$M < 2^{2m}.$$

Hierzu ist es sinnvoll, den Binomischen Lehrsatz anzuwenden:

$$2^{2m+1} = \sum_{k=0}^{2m+1} \binom{2m+1}{k} > \binom{2m+1}{m+1} + \binom{2m+1}{m} = 2M.$$

Wenn

$$m+1 < p \leq 2m+1$$

gilt, teilt p den Zähler, da dieser nichts anderes als das Produkt dieser p ist, jedoch nicht den Nenner von M, da p prim, somit

$$\left(\prod_{m+1<p\leq 2m+1} p \right) \mid M.$$

Insgesamt folgt damit

$$\Theta(2m+1) - \Theta(m+1) = \sum_{m+1<p\leq 2m+1} \log(p) \leq \log(M) < 2m \log(2).$$

Die erste Gleichheit folgt unmittelbar aus der Definition von $\Theta(x)$. Die darauf folgende Abschätzung beruht darauf, dass die Summe von Logarithmen gleich dem Logarithmus des Produkts ist. Die letzte Abschätzung schließen wir aus der zuvor bewiesenen Tatsache, dass $M < 2^{2m}$.

Wir beweisen nun $(**)$ per Induktion. $(**)$ ist für $n = 1$ und $n = 2$ trivial. Angenommen es gilt für jedes $n \leq n_0 - 1$. Für n_0 gerade gilt:

$$\Theta(n_0) = \Theta(n_0 - 1) < 2(n_0 - 1)\log(2) < 2n_0 \log(2).$$

Die erste Gleichheit gilt, weil bei $\Theta(x)$ für gerades n_0 gegenüber dem ungeraden $n_0 - 1$ kein Summand hinzukommt, da Primzahlen nicht gerade sein können. Die darauf folgende Abschätzung nutzt die Induktionsvoraussetzung. Für n_0 ungerade gilt:

$$\begin{aligned}\Theta(n_0) &= \Theta(2m+1) = \Theta(2m+1) - \Theta(m+1) + \Theta(m+1) \\ &< 2m\log(2) + 2(m+1)\log(2) = 2(2m+1)\log 2 = 2n_0\log(2),\end{aligned}$$

da bei der Substitution $n_0 = 2m + 1$ gilt $m + 1 < n_0$. Die erste Abschätzung nach oben nutzt die Induktionsvoraussetzung und die oben bewiesene Abschätzung für $\Theta(2m + 1) - \Theta(m + 1)$.
Induktiv folgt somit $(**)$.

Die Zahlen $1, 2, ..., n$ enthalten höchstens $\lfloor \frac{n}{p} \rfloor$ Vielfache von p, höchstens $\lfloor \frac{n}{p^2} \rfloor$ Vielfache von p^2, etc. Daraus folgt die Gleichheit:

$$n! = \prod_p p^{\sum_{m \geq 1} \lfloor \frac{n}{p^m} \rfloor}. \qquad (***)$$

Dazu ein Beispiel: Für $n = 5$ durchlaufen wir das Produkt für $p = 2, 3, 5$. Für $p = 2$ finden wir $m = 1$ und $m = 2$, sodass $p = 2$ den Exponenten $\lfloor \frac{5}{2} \rfloor + \lfloor \frac{5}{4} \rfloor = 3$ hat. Analog hat $p = 3$ den Exponenten $\lfloor \frac{5}{3} \rfloor = 1$ und $p = 5$ den Exponenten $\lfloor \frac{5}{5} \rfloor = 1$. Gemeinsam ergibt sich $2^3 * 3^1 * 5^1 = 2 * 3 * 4 * 5 = 5!$.
Wir schreiben

$$N = \frac{(2n)!}{(n!)^2} = \prod_{p \leq 2n} p^{k_p},$$

sodass nach $(***)$:

$$k_p = \sum_{m=1}^{\infty} \left(\lfloor \frac{2n}{p^m} \rfloor - 2 \lfloor \frac{n}{p^m} \rfloor \right).$$

Hierzu kürzen wir bei N im Zähler und Nenner ein $n!$ und wenden auf $(***)$ grundlegende Potenzgesetze an. Die Summanden sind jeweils gleich 1 oder 0, je nachdem, ob $\lfloor \frac{2n}{p^m} \rfloor$ ungerade oder gerade ist. Alternativ betrachtet sind alle Summanden mit $p^m > 2n$ gleich 0, sonst 1. Daraus folgt:

$$k_p \leq \frac{\log(2n)}{\log(p)},$$

da die Summanden für $p^m \leq 2n \iff m \leq \frac{\log(2n)}{\log(p)}$ gleich 1 sind. Ab dieser Grenze werden die Summanden gleich 0, daher die Abschätzung.
Insgesamt folgt:

$$\log(N) = \sum_{p\leq 2n} k_p \log(p) \leq \sum_{p\leq 2n} \frac{\log(2n)}{\log(p)} \log(p) = \Psi(2n).$$

Die erste Gleichheit folgt erneut daraus, dass der Logarithmus eines Produkts die Summe der Logarithmen ist. Die darauf folgende Abschätzung wurde oben bewiesen. Durch Kürzen von $\log(p)$ bleibt die Definition von $\Psi(x)$ für $x = 2n$.
Wir schätzen nun N mit $N = \frac{(2n)!}{(n!)^2} = \frac{n+1}{1} * \frac{n+2}{2} * ... * \frac{2n}{n} \geq 2^n$ ab, dabei wird für die erste Gleichheit $n!$ gekürzt, die darauf folgende Abschätzung kann induktiv mittels des Binomischen Lehrsatzes gezeigt werden.
Abschließend erhalten wir

$$\Psi(2n) \geq \log(N) \geq \log(2^n) = n\log(2),$$

woraus mit $n = \frac{x}{2}$ direkt $(*)$ folgt. [1, S. 341,342] [6, S. 60,61,62]

4.4.3 $\pi(x) \asymp \frac{\Theta(x)}{\log(x)} \asymp \frac{\Psi(x)}{\log(x)}$

Wegen

$$\Theta(x) = \sum_{p\leq x} \log(p) \leq \log(x) \sum_{p\leq x} 1 = \pi(x)\log(x)$$

folgt, nachdem $\Theta(x) \asymp x$ bewiesen wurde, $\pi(x) \geq \frac{\Theta(x)}{\log(x)} > \frac{Ax}{\log(x)}$. Außerdem führen wir die folgende Abschätzung durch:

$$\begin{aligned}\Theta(x) \geq & \sum_{x^{1-d}<p\leq x} \log(p) \geq (1-d)\log(x) \sum_{x^{1-d}<p\leq x} 1 \\ &= (1-d)\log(x)(\pi(x) - \pi(x^{1-d})) \geq (1-d)\log(x)(\pi(x) - x^{1-d}).\end{aligned}$$

Die erste Abschätzung folgt unmittelbar aus der Definition von $\Theta(x)$. Stellen wir $x^{1-d} < p \leq x$ nach d um, erhalten wir $d \geq 0$. d ist eine positive Konstante, mittels derer wir die Beschränktheit zeigen können. Bei der letzten Abschätzung ist das Minus zu beachten, hier wird die Eigenschaft $\pi(x) \leq x$ genutzt.

Teilen wir das Resultat $\Theta(x) \geq (1-d)\log(x)(\pi(x) - x^{1-d})$ durch $(1-d)\log(x)$ und bringen x^{1-d} auf die linke Seite, folgt

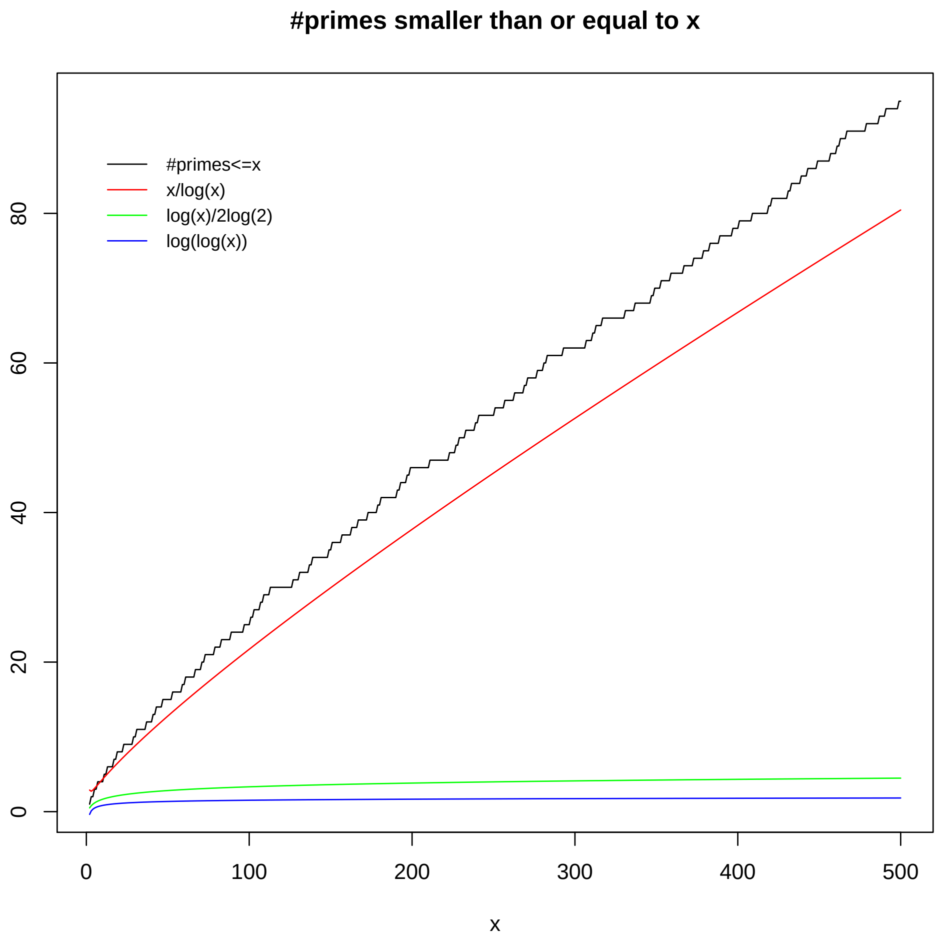
$$\pi(x) \leq x^{1-d} + \frac{\Theta(x)}{(1-d)\log(x)} < \frac{Bx}{\log(x)}.$$

[1, S. 345]
Wir haben damit bewiesen, dass A und B existieren, sodass

$$\frac{Ax}{\log(x)} < \pi(x) < \frac{Bx}{\log(x)}.$$

$\square$

Wir schließen das Kapitel mit einer von mir in R programmierten Grafik, die das asymptotische Verhalten der drei Funktionen im Vergleich zu $\pi(x)$ verdeutlicht.



Kapitel 5

Ausblick

Wir haben in dieser Arbeit einen Schnelldurchlauf der letzten Jahrtausende erlebt, wie sich die Approximation der Dichte der Primzahlen entwickelt hat. Wir konnten unter Hinzunahme diverser Sätze, Definitionen und Zahlenfolgen zeigen, dass sich die Menge der Primzahlen $\pi(x)$ asymptotisch äquivalent zu der Funktion $\frac{x}{ln(x)}$ verhält. Interessant wäre nun zu sehen, welchen weiteren Verlauf entsprechende Approximationen noch nehmen. So kann man beweisen, dass der Integrallogarithmus $Li(x) := \int_2^x \frac{dt}{ln(t)}$ eine bessere Approximation als $\frac{x}{\log(x)}$ darstellt. Er ist asymptotisch äquivalent zu $\frac{x}{\log(x)}$ und somit auch zu $\pi(x)$, der Beweis hierzu baut auf dieser Arbeit auf. Lowell Schoenfeld fand unter Annahme der Riemann-Vermutung sogar eine nicht-asymptotische Schranke $|\pi(x) - Li(x)| < \frac{\sqrt{x} ln(x)}{8\pi}$.

Wir haben in dieser Arbeit gelernt, dass $\frac{x}{\log(x)}$ die richtige Größenordnung für $\pi(x)$ hat. Nun gilt es, wie bereits in der Einleitung angekündigt, zu beweisen, dass $\frac{\pi(x)}{\frac{x}{\log(x)}} \longrightarrow 1$ gilt. Dieser Beweis sei nun jedem als Übung selbst überlassen.

Erklärung

gemäß § 18 Abs. 6 und § 15 Abs. 8 der Ordnung für die Prüfung im lehramtsbezogenen Bachelorstudiengang an der Johannes Gutenberg-Universität Mainz (POLBA, ggf. POLBA-Dijon), bzw. § 18 Abs. 5 und § 15 Abs. 10 der Ordnung für die Prüfung im Masterstudiengang für das Lehramt an Gymnasien (POLMA, ggf. POLMA Dijon, iPOLMA-Dijon).

Hiermit erkläre ich, ______________________________________ (Matr.-Nr.: _________________________), dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen oder Hilfsmittel (einschließlich elektronischer Medien und Online-Quellen) benutzt habe. Mir ist bewusst, dass ein Täuschungsversuch oder ein Ordnungsverstoß vorliegt, wenn sich diese Erklärung als unwahr erweist. § 18 Abstatz 3 und 4 der o. g. Ordnungen gilt in diesem Fall entsprechend.

______________________ ______________________

Ort, Datum Unterschrift

Literaturverzeichnis

[1] Hardy, G. H. ; Wright, E. M. : An Introduction to the Theory of Numbers. New York, London: OUP Oxford, 1960.

[2] Aigner, Martin ; Ziegler, Günter M.: Das BUCH der Beweise. Berlin Heidelberg New York: Springer-Verlag, 2014.

[3] Böhm, Janko: Grundlagen der Algebra und Zahlentheorie. Berlin Heidelberg New York: Springer-Verlag, 2016.

[4] Laures, Gerd ; Szymik, Markus : Grundkurs Topologie. Berlin Heidelberg: Springer-Verlag, 2015.

[5] Holzapfel, Michael : Anzahl von Primzahlen. Unter: http://www.michael-holzapfel.de/themen/primzahlen/pz-anzahl.htm (abgerufen am 21.04.2018).

[6] O'Rourke, Ciarán: The prime number theorem: Analytic and elementary proofs. Unter: eprints.maynoothuniversity.ie/4470/1/finaldraftmsc.pdf (abgerufen am 21.04.2018).