TECHNISCHE UNIVERSITÄT WIEN

# Diplomarbeit

# Anzahlsätze für Primzahlen und Primzahlkonstellationen

ausgeführt am Institut für

Algebra und Computermathematik

der Technischen Universität Wien

unter der Anleitung von
a.o.Univ.Prof. Dipl.Ing. Dr.techn. Johann Wiesenbauer

durch

Georg Gutenbrunner

Greinerstraße 21
A - 4320 Perg

Breitenfeldergasse 9/17
A - 1080 Wien

Februar 2002

# Vorwort

*„Die Lehre von der Verteilung der Primzahlen*
*ist als eines der* allerwichtigsten *Kapitel*
*der mathematischen Wissenschaft anzusehen...“*
*[Lan09a]*

Primzahlen gehören wohl zum Faszinierendsten, was die Mathematik zu bieten hat und haben zu allen Zeiten sowohl Mathematiker, als auch Laien in ihren Bann gezogen. Tatsächlich zeichnen sich die Probleme auf dem Gebiet der Primzahlen durch besondere Einfachheit und einzigartige Eleganz in ihrer Beschreibung und Formulierung aus.

Und dennoch: nur all zu oft verbirgt sich hinter den spielerisch anmutenden Problemstellungen eine im wahrsten Sinne des Wortes „undenkbare“ Komplexität in den Details. Die Grundbegriffe, die für die Definition der Primzahlen notwendig sind, lassen sich jedem Kind leicht beibringen. Trotzdem gibt es unzählige Beispiele, die den menschlichen Geist weit zu übersteigen scheinen.

Den Problemen in der Theorie der Primzahlen ist es zu eigen, dass sie sich oft lange Zeit hartnäckig jedem Versuch der „Erledigung“, wie es Landau vor knapp 100 Jahren formulierte, entgegensetzen. Es hat überdies den Anschein, als würde die intensive Forschung auf dem Gebiet der Primzahlen mehr neue Fragen aufwerfen, denn alte lösen. Seit sich Euler in der Mitte des 18. Jahrhunderts als erster nach Euklid (der immerhin 2000 Jahre vorher lebte) wieder mit den Primzahlen beschäftigte, sind eine Reihe wichtiger Probleme nach und nach gelöst worden. Einige jedoch hielten selbst den Bemühungen zahlreicher bedeutender Mathematiker bis jetzt stand.

Dies trifft auch auf die folgenden drei großen Vermutungen zu, die in der vorliegenden Arbeit eine bedeutsame Rolle spielen. Das erste Resultat stellt in mehrfacher Hinsicht etwas Besonderes unter diesen dar. 1994 konnten An-

drew Wiles und Richard Taylor nach jahrelangen Forschungen eine über 300 Jahre alte Vermutung endlich beweisen.

**Satz 1 (Der große Fermat)** *Es gibt für $n \geq 3$ keine ganzzahligen Lösungen $x, y, z \in \mathbb{Z} \setminus \{0\}$, mit*

$$x^n + y^n = z^n. \tag{1}$$

Dieser Satz aus dem Jahre 1670 hat zunächst auf den ersten Blick unmittelbar gar nichts mit Primzahlen zu tun. In den vielen Beweisversuchen seither wurde Satz 1 für Spezialfälle immer wieder gelöst. Dabei entstanden interessante Definitionen von Primzahlen spezieller Bauart, wie sie in Kapitel 2 genauer untersucht werden.

Rund 70 Jahre später, zu der Zeit also, wo Euler sich mit den Primzahlen beschäftigte, war es der Mathematiker Goldbach, der in einem Brief vom 7.Juli 1742 an Euler die zweite große Vermutung äußerte:

**Vermutung 2 (Goldbach'sche Vermutung)** *Jede gerade natürliche Zahl $n \geq 4$ ist als Summe von zwei Primzahlen $p, q \in \mathbb{P}$ darstellbar:*

$$n = p + q. \tag{2}$$

Wie der Name schon sagt, ist sie nach wie vor unbewiesen, und das seit immerhin 260 Jahren! Es gibt auch hier Ergebnisse für manche Spezialfälle, die durch enormen Aufwand erzielt wurden, jedoch steht der große Durchbruch noch aus. Nicht zuletzt um diese Vermutung endlich zu entscheiden, wurden im Laufe der Zeit neue, höchst komplizierte Siebmethoden entwickelt. Sie stellen aus heutiger Sicht das aussichtsreichste Mittel dar, um die Vermutung 2 zu beweisen. Im Jahre 1919 brachten die Anstrengungen rund um das Sieben ein wichtiges Ergebnis durch Viggo Brun hervor, mit dem sich Teile des letzen Kapitels beschäftigen werden.

Die letzte der oben angesprochenen Vermutungen entstand wiederum rund 120 Jahre später und ist nach dem Urteil vieler Mathematiker das herausragendste ungelöste Problem der Mathematik. Ihre Bedeutung ergibt sich aus wichtigen Folgerungen für die verschiedensten Teilgebiete der Mathematik.

**Vermutung 3 (Riemann'sche Vermutung)** *Die Nullstellen der Riemann'schen Funktion $\zeta(s)$ im kritischen Streifen $0 < \mathrm{Re}(s) < 1$ liegen alle auf der Mittelgeraden $\mathrm{Re}(s) = \frac{1}{2}$.*

Sie wird in Kapitel 3, zusammen mit Eigenschaften von $\zeta(s)$, etwas eingehender untersucht.

Bevor jedoch das Augenmerk auf Riemann und seine wertvollen Beiträge zur Zahlentheorie gerichtet wird, werden zunächst in einem einleitenden Kapitel einige grundlegende Begriffe eingeführt, soweit sie in den anschließenden Kapiteln, welche von Anzahlsätzen für Primzahlen und Primzahlkonstellationen handeln, verwendet werden.

Mit Hilfe einfachster Mittel werden im zweiten Kapitel erste elementare Resultate zu Primzahlen behandelt und ausgewählte Sätze auch bewiesen. Dies gilt etwa für das klassische Ergebnis von Euklid, für dessen Beweis zwei verschiedene Varianten angegeben werden.

Anschließend werden spezielle Primzahlarten ausführlich untersucht. Darunter sind natürliche Zahlen gemeint, die nach einem gewissen Muster gebildet werden, und die prim sind. Neben den bekanntesten beiden Typen solcher Zahlen, den Fermat'schen Zahlen $F_n$ und den Mersenne'schen Zahlen $M_n$, werden auch drei Arten von Primzahlen behandelt, die aus den Beweisversuchen von Satz 1 hervorgegangen sind. Aus Platzgründen können jedoch nicht alle verschiedenen bekannten Primzahlarten untersucht werden.

In einem letzten Abschnitt werden noch weitere interessante Fragestellungen behandelt, und ein Beweis des Bertrand'schen Postulates 2.3.1 angegeben.

In Kapitel 3 schließlich wird das Verständnis über die Riemann'sche $\zeta$-Funktion vertieft und auf ihre Rolle in der Primzahlverteilung eingegangen. In diesem Zusammenhang werden ausführliche Rechnungen mit den Nullstellen von $\zeta(s)$ angestellt, wobei die von DERIVE gebotene Möglichkeit, die Stellenanzahl beliebig zu erhöhen, von großem Nutzen ist.

Weiters wird der große Primzahlsatz 3.2.1 samt seiner geschichtlichen Entwicklung vorgestellt. Für einen Beweis muss aus Platzgründen auf die Literatur verwiesen werden.

Das Ende des Kapitels ist der Funktion $\pi(x)$, welche die Primzahlen kleiner oder gleich $x$ abzählt, gewidmet. Es existieren mehrere Verfahren, $\pi(x)$ auch ohne Kenntnis der einzelnen Primzahlen zu approximieren bzw. zu berechnen. Den Abschluss stellt eine Implementierung der zuvor entwickelten Ideen in DERIVE dar.

Das vierte Kapitel stellt ganz kurz das Analogon von 3.2.1 für Primzahlen in arithmetischen Folgen vor. Wieder kann, nicht zuletzt aus Gründen der komplexen Theorie dahinter, kein Beweis dieses Satzes - von zwei Spezialfällen abgesehen - angegeben werden.

Schließlich wird noch ausführlich auf die Primzahlkonstellationen eingegangen. Zunächst werden einleitend einige Begriffe entwickelt, ehe die Primzahlzwillinge als einfachste und wohl auch bekannteste Konstellation genauer untersucht werden.

Auf die Arbeit von Hardy und Littlewood [HL22] aufbauend, wird für mehrere Beispiele von Primzahlkonstellationen eine Approximation ihrer Anzahl aufgestellt, wobei auch wieder DERIVE zum Einsatz kommt.

Quer durch die gesamte Diplomarbeit tauchen immer wieder DERIVE - Programme auf, die dem besseren Verständnis der Materie dienlich sein sollen. Darum findet sich auch im Anhang ein Verzeichnis verwendeter eingebauter Funktionen, sowie der selbst programmierten Routinen. Die meisten dieser kurzen Programme sind sehr einfach aufgebaut und als Modelllösungen zu verstehen, die auch noch je nach Bedarf ausgebaut werden können. Zum Teil wird bei den Funktionen ein sinnvoller Input vorausgesetzt, da auf die notwendigen Abfragen zu Gunsten der Lesbarkeit verzichtet wurde. Die Berechnungen wurden in DERIVE 5.05 auf einem Pentium III mit 600 MHz durchgeführt. Die Rechenzeiten sind dementsprechend zu interpretieren.

Neben einem ausführlichen Literaturverzeichnis am Ende der Arbeit, wurde auch auf eine Liste der Internet-Seiten ein besonderes Augenmerk gerichtet. Mathematiker sind weltweit rund um die Uhr bemüht, das eine oder andere Geheimnis über Primzahlen zu lüften. Das Internet bietet eine einfache Möglichkeit, sich laufend auf dem neuesten Stand der Wissenschaft zu halten. Die angeführten Adressen sollen dabei eine kleine Hilfestellung bieten, um sich auf der Suche nach einschlägigen Informationen im Internet leichter zurechtzufinden.

Georg Gutenbrunner

Februar 2002

# Inhaltsverzeichnis

# Kapitel 1

# Mathematische Grundlagen

## 1.1 Grundbegriffe aus der Zahlentheorie

In Arbeiten auf dem Gebiet der Zahlentheorie scheint es besonders wichtig zu sein, die Menge $\mathbb{N}$ der natürlichen Zahlen zu „definieren“. In dieser Diplomarbeit wird unter $\mathbb{N}$ stets die folgende Menge

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}, \tag{1.1}$$

verstanden. Statt $\mathbb{N} \setminus \{0\}$ schreibt man auch

$$\mathbb{N}^{\times} = \{1, 2, 3, \ldots\}. \tag{1.2}$$

Weiters seien die Begriffe $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ als Menge der ganzen, rationalen, reellen bzw. der komplexen Zahlen definiert. Der Vollständigkeit halber sei hier auch noch die Menge $\mathbb{P}$ angemerkt, die in der Definition 2.1.1 ohnedies als Menge der Primzahlen eingeführt wird.

In der Zahlentheorie tauchen immer wieder verschiedene Klammer-Arten auf, die wir an dieser Stelle definieren wollen:

**Definition 1.1.1** *Sei $a$ eine beliebige Zahl, dann bezeichnet*

$$\lfloor a \rfloor = [a] \tag{1.3}$$

*die nächstkleinere ganze Zahl zu $a$, und*

$$\lceil a \rceil \tag{1.4}$$

*die nächstgrößere ganze Zahl zu $a$. Damit folgt unmittelbar*

$$\lfloor a \rfloor + 1 = \lceil a \rceil \qquad \textit{bzw.} \qquad \lfloor a \rfloor = \lceil a \rceil - 1. \tag{1.5}$$

Weiters wird bei einem Beweis von Satz 2.1.2 ein zentrales Ergebnis der elementaren Zahlentheorie benötigt:

**Satz 1.1.2 (Fundamentalsatz der Zahlentheorie)** *Sei $n$ eine beliebige natürliche Zahl, und seien die Primzahlen in beliebiger, aber fester Art und Weise durchnummeriert: $p_1, p_2, \ldots$ (z.B. $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$). Dann lässt sich $n$ als Produkt von (endlich vielen) Primzahlen $p_1, \ldots, p_s$ schreiben*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} = \prod_{i=1}^{s} p_i^{\alpha_i}. \tag{1.6}$$

*Dabei gilt $\alpha_i \in \mathbb{N}$. Weiters ist diese Darstellung in folgendem Sinn eindeutig:*

$$n = \prod_{i=1}^{s} p_i^{\alpha_i} = \prod_{i=1}^{t} p_i^{\beta_i} \Rightarrow s = t \tag{1.7}$$

*und*

$$\alpha_i = \beta_i, i = 1, \ldots, s. \tag{1.8}$$

*Beweis:* Siehe etwa [HW58], §2.10, §2.11. □

Darüberhinaus soll nachstehende Schreibweise eingeführt werden:

**Definition 1.1.3** *Bezeichne* $\mathrm{ggT}(a, n)$ *den größten positiven Teiler $d$ von $a$ und $n$. Dann gilt*

$$(a, n) = 1 \Leftrightarrow \mathrm{ggT}(a, n) = 1. \tag{1.9}$$

*Zahlen $a$ und $n$ mit $(a, n) = 1$ heißen* teilerfremd.

Wenn also aus dem Zusammenhang hervorgeht, dass man mit $(.,.)$ kein geordnetes Paar versteht, dann ist der größte gemeinsame Teiler der beiden Elemente in $(.,.)$ gemeint.

Um den nächsten Satz formulieren zu können, muss ihm eine Definition vorangestellt werden:

**Definition 1.1.4 (Euler-Gamma)** *Das Euler-Gamma ist wie folgt definiert:*

$$\gamma := \lim_{N \to \infty} \left( \sum_{n=1}^{N} \frac{1}{n} - \ln N \right) \approx 0.5772156649. \tag{1.10}$$

Damit gilt der Satz

**Satz 1.1.5 (Satz von Mertens)** *Bezeichne $p$ eine Primzahl, und $\gamma$ das Euler-Gamma, dann gilt für $x \to \infty$*

$$\prod_{2 \leq p \leq x} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\ln x} \approx \frac{0.5615}{\ln x}. \tag{1.11}$$

*Beweis:* Siehe etwa [HW58], §22.8.

□

Unter der Bezeichnung „$a$ ist quadratischer Rest mod $p$“ versteht man, dass ein $x$ existiert, sodass $x^2 \equiv a(p)$ gilt. Existiert hingegen kein solches $x$, so wird $a$ „quadratischer Nichtrest mod $p$“ genannt. In diesem Sinne ist die folgende Definition zu verstehen.

**Definition 1.1.6 (Legendre-Symbol)** *Sei $p > 2$ eine Primzahl, $a \in \mathbb{Z}$; das quadratische Restsymbol nach Legendre ist definiert durch:*

$$\left(\tfrac{a}{p}\right) = \begin{cases} 1 & \dots \quad a \text{ ist quadratischer Rest mod } p \\ 0 & \dots \quad p \mid a \\ -1 & \dots \quad a \text{ ist quadratischer Nichtrest mod } p \end{cases}$$

Mit Hilfe dieses Symbols kann man oft sehr leicht das Gebiet der quadratischen Reste untersuchen. Ein wichtiges Resultat in diesem Zusammenhang ist das sogenannte „quadratische Reziprozitätsgesetz“, zu dem es zwei Ergänzungssätze gibt.

**Satz 1.1.7 (Quadratisches Reziprozitätsgesetz)** *Seien $p, q$ Primzahlen, beide größer 2, dann gilt:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{1.12}$$

**Satz 1.1.8 (Erster Ergänzungssatz)** *Sei $p > 2$ Primzahl, dann gilt*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}. \tag{1.13}$$

*Es ist also $-1$ genau dann quadratischer Rest mod $p$, wenn $p \equiv 1(4)$, und quadratischer Nichtrest mod $p$, wenn $p \equiv 3(4)$ ist.*

**Satz 1.1.9 (Zweiter Ergänzungssatz)** *Sei $p > 2$ Primzahl, dann gilt*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \tag{1.14}$$

*Es ist also 2 genau dann quadratischer Rest mod $p$, wenn $p \equiv \pm 1(8)$, und quadratischer Nichtrest mod $p$, wenn $p \equiv \pm 3(8)$ ist.*

Nun noch zum Begriff der zahlentheoretischen Funktion.

**Definition 1.1.10 (Zahlentheoretische Funktion)** *Unter einer zahlentheoretischen Funktion $f$ versteht man eine Funktion, deren Definitionsbereich gleich der Menge der natürlichen Zahlen $\mathbb{N}^\times$ ist, und die in die Menge der komplexen Zahlen abbildet:*

$$f : \mathbb{N}^\times \to \mathbb{C} \tag{1.15}$$

Als Beispiel einer zahlentheoretischen Funktion sei hier die Teilersummenfunktion $\sigma$ angeführt, die wie folgt definiert ist:

$$\sigma(n) := \sum_{d|n} d. \tag{1.16}$$

Aber es tauchen auch andere Beispiele im Zuge der Arbeit auf, etwa:

**Definition 1.1.11 (Euler'sche $\varphi$-Funktion)** *Unter der zahlentheoretischen Funktion $\varphi : \mathbb{N}^\times \to \mathbb{N}^\times$ versteht man jene Abbildung, die der natürlichen Zahl $n \neq 0$ die Anzahl der zu $n$ teilerfremden Zahlen $\leq n$ zuordnet:*

$$\varphi(n) := |\{m \in \mathbb{N}^\times, m \leq n | \operatorname{ggT}(m,n) = 1\}|. \tag{1.17}$$

*Man nennt $\varphi$ auch* Euler'sche $\varphi$-Funktion.
*Vom algebraischen Standpunkt aus betrachtet, bezeichnet $\varphi(p)$ also die Kardinalität der multiplikativen Einheitengruppe $\mathbb{Z}_p^*$.*

Abschließend wollen wir noch zur „Dickman-Funktion“ kommen, wozu wir zunächst weitere Begriffe einführen müssen.

**Definition 1.1.12** *Eine natürliche Zahl $n$ heißt „$y$-glatt“, wenn $n$ keinen Primteiler hat, der größer $y$ ist.*
*Diese Zahlen werden durch folgende Funktion abgezählt:*

$$\psi(x,y) := |\{1 \leq n \leq x | n \text{ ist } y\text{-glatt}\}|. \tag{1.18}$$

Von Dickman gibt es aus dem Jahre 1930 einen Satz, in dem die gesuchte Funktion vorkommt:

**Satz 1.1.13 (Dickman)** *Für jede feste reelle Zahl $u > 0$ gibt es eine reelle Zahl $\rho(u) > 0$, so dass*

$$\psi(x, x^{1/u}) \sim \rho(u)x. \tag{1.19}$$

Dickman beschreibt diese Funktion $\rho(u) : [0, \infty) \to \mathbb{R}$ als Lösung einer speziellen Differentialgleichung:

1. $\rho(u) = 1$ für $0 \leq u \leq 1$

2. $\rho'(u) = -\frac{\rho(u-1)}{u}$.

Für $1 \leq u \leq 2$ gilt: $\rho(u) = 1 - \ln u$, jedoch ist für größere $u$ keine geschlossene Form bekannt. $\rho(u)$ kann numerisch approximiert werden, und es stellt sich heraus, dass sie sehr rasch gegen Null konvergiert, rascher als $u^{-u}$, auch wenn letzteres oft als Abschätzung in der Komplexitätstheorie verwendet wird. Tatsächlich gilt

$$\ln \rho(u) \sim -u \ln u. \tag{1.20}$$

## 1.2 Grundlagen aus der Analysis

Die nachstehenden Landau'schen Symbole finden in dieser Arbeit häufig Verwendung, weshalb sie ihr vorangestellt werden.

**Definition 1.2.1 (Landau-Symbole)** *Seien im Folgenden $f(n)$ und $g(n)$ stets reelle Funktionen auf der Menge der natürlichen Zahlen. Dann definiert man folgende Menge*

$$O(g(n)) := \{f(n) | \exists C > 0, n_0 \in \mathbb{N} : |f(n)| \leq C|g(n)| \ \forall n \geq n_0\} \tag{1.21}$$

*als die Menge aller Funktionen $f(n)$, die höchstens so rasch wachsen wie $g(n)$. Für $f(n) \in O(g(n))$ schreibt man kurz*

$$f(n) = O(g(n)). \tag{1.22}$$

*Mathematisch gesehen bedeutet dies*

$$\limsup_{n \to \infty} \frac{|f(n)|}{g(n)} < \infty, \tag{1.23}$$

*es gibt also eine Konstante $C$, sodass für hinreichend großes $n$*

$$|f(n)| < Cg(n) \tag{1.24}$$

*gilt. Darüberhinaus betrachtet man auch*

$$\Omega(g(n)) := \{f(n) | \exists C > 0, n_0 \in \mathbb{N} : |f(n)| \geq C|g(n)| \ \forall n \geq n_0\}, \tag{1.25}$$

*die Menge all jener Funktionen $f(n)$, die mindestens so rasch wie $g(n)$ wachsen. Es gilt*

$$f(n) = \Omega(g(n)) \Leftrightarrow \liminf_{n\to\infty} \frac{|f(n)|}{g(n)} > \infty. \tag{1.26}$$

*Weiters ist folgende Definition wichtig:*

$$\Theta(g(n)) := O(g(n)) \cap \Omega(g(n)) = \{f(n) | f(n) = O(g(n)) \wedge f(n) = \Omega(g(n))\}. \tag{1.27}$$

*In der bisherigen Schreibweise bedeutet das also*

$$\Theta(g(n)) = \{f(n) | \exists C_1, C_2 > 0, n_0 \in \mathbb{N} : C_1|g(n)| \leq |f(n)| \leq C_2|g(n)| \; \forall n \geq n_0\}. \tag{1.28}$$

*Für die Praxis gilt*

$$\lim_{n\to\infty} \frac{|f(n)|}{|g(n)|} = C, C > 0 \Rightarrow f(n) = \Theta(g(n)). \tag{1.29}$$

*Im Spezialfall von $C = 1$ schreibt man auch $f(n) \sim g(n)$ und sagt, die beiden Funktionen seien „asymptotisch gleich". Schließlich führen wir der Vollständigkeit halber noch die beiden letzten Schreibweisen an:*

$$f(n) = o(g(n)) :\Leftrightarrow \lim_{n\to\infty} \frac{|f(n)|}{|g(n)|} = 0, \tag{1.30}$$

*also „$f(n)$ wächst langsamer als $g(n)$", bzw.*

$$f(n) = \omega(g(n)) :\Leftrightarrow \lim_{n\to\infty} \frac{|f(n)|}{|g(n)|} = \infty, \tag{1.31}$$

*„$f(n)$ wächst schneller als $g(n)$".*

Unter Verwendung der folgenden Eigenschaft des natürlichen Logarithmus, lässt sich Satz 2.1.4 zeigen.

**Lemma 1.2.2** *Es gelte $-1 \leq x < 1$, dann gilt folgende Potenzreihenentwicklung*

$$\ln(1 - x) = -\sum_{i=1}^{\infty} \frac{x^i}{i}. \tag{1.32}$$

Zu Beginn der Untersuchungen der Riemann'schen $\zeta$-Funktion in Kapitel 3 taucht der Begriff der Gamma-Funktion $\Gamma(s)$ auf:

**Definition 1.2.3** *Unter der Gamma-Funktion* $\Gamma(s), s \in \mathbb{C}, \mathrm{Re}(s) > 0$, *versteht man folgende Funktion*

$$\Gamma(s) := \int_0^\infty x^{s-1} e^{-x}\, dx. \tag{1.33}$$

*Durch mehrfache Anwendung der Funktionalgleichung*

$$\Gamma(s+1) = s\Gamma(s) \tag{1.34}$$

*kann man ihren Definitionsbereich beliebig nach links vergrößern. Als ihre einzigen Pole erhält man die nichtpositiven ganzen Zahlen* $0, -1, -2, \ldots$. *Sämtliche Pole sind von erster Ordnung.*

Um den Satz 5.2.2 zu erhalten, benötigen wir schließlich das folgende

**Lemma 1.2.4**

$$\begin{aligned} \sum_{2 \le n \le x} \frac{1}{n \ln^2 n} &= \int_2^x \frac{du}{u \ln^2 u} + c' + O\left(\frac{1}{x \ln^2 x}\right) \\ &= -\frac{1}{\ln x} + c + O\left(\frac{1}{x \ln^2 x}\right). \end{aligned} \tag{1.35}$$

# Kapitel 2

# Primzahlen

## 2.1 Erste elementare Ergebnisse

### 2.1.1 Der Satz von Euklid

„Am Anfang war die Primzahl...“ könnte man in Anlehnung an das berühmte Bibelwort sagen, und so wollen wir es halten, und beginnen zunächst mit der allseits bekannten Definition der Primzahl, dem fundamentalen Begriff in dieser Arbeit.

**Definition 2.1.1 (Primzahl)** *Eine natürliche Zahl $p \in \mathbb{N}, p \geq 2$ wird als prim bezeichnet, wenn die Menge ihrer positiven natürlichen Teiler in $\mathbb{N}$ nur die Zahlen 1 und $p$ selbst, die sogenannten* trivialen Teiler*, enthält.*
*Eine prime Zahl wird auch* Primzahl *genannt, und die Menge aller Primzahlen wird mit $\mathbb{P}$ bezeichnet.*

Führt man in der Mathematik einen neuen Begriff ein, so sollte man sich stets davon überzeugen, dass die geforderten Eigenschaften nicht zu einschränkend sind, dass also noch Objekte existieren, die der neuen Definition genügen. Andernfalls besteht die Möglichkeit, dass sich sämtliche weiterführenden Untersuchungen auf die leere Menge $\emptyset$ beziehen, aus der bekanntlich allerlei Falsches hergeleitet werden kann.

Diese Gefahr scheint bei dem Begriff der Primzahl gebannt, gilt doch:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, \ldots \in \mathbb{P}$$

Die Menge $\mathbb{P}$ der Primzahlen ist demnach nicht leer. Im Gegenzug kann man sich nun die Frage stellen, wieviele natürliche Zahlen die Eigenschaft, prim zu sein, besitzen. Dazu zunächst eine heuristische Überlegung:

Sei $n \in \mathbb{N}$ eine beliebige, fest gewählte natürliche Zahl. Die Wahrscheinlichkeit, dass $n$ durch eine natürliche Zahl $d \leq n$ geteilt wird, ist $\frac{1}{d}$. Die Gegenwahrscheinlichkeit, dass also $d \nmid n$ gilt, ergibt sich somit zu $1 - \frac{1}{d} = \frac{d-1}{d} < 1$. Weiters besitzt jede zusammengesetzte Zahl $m$ wenigstens einen Primfaktor kleiner oder gleich $\sqrt{m}$. Somit ergibt sich unter der Annahme, dass die Teilbarkeit durch verschiedene Primzahlen jeweils voneinander unabhängige Ereignisse sind, für die Wahrscheinlichkeit, dass $n$ prim ist, folgender Ausdruck:

$$\mathcal{W}(n \in \mathbb{P}) = \prod_{p \in \mathbb{P}, p \leq \sqrt{n}} \left(1 - \frac{1}{p}\right) \tag{2.1}$$

Aus dem Primzahlsatz 2.1.9 folgt unmittelbar, dass diese Wahrscheinlichkeit für ein großes, zufällig gewähltes $x$ ungefähr gleich $\frac{1}{\ln x}$ sein sollte, also insgesamt

$$\prod_{2 \leq p \leq x^{0.5}} \left(1 - \frac{1}{p}\right) \sim \frac{1}{\ln x} \qquad x \to \infty. \tag{2.2}$$

Dies widerspricht jedoch dem Satz von Mertens 1.1.5, wonach folgende Näherung gilt

$$\prod_{2 \leq p \leq x^{0.5615}} \left(1 - \frac{1}{p}\right) \sim \frac{1}{\ln x} \qquad x \to \infty. \tag{2.3}$$

Diese Diskrepanz muss in der Tatsache begründet sein, dass es Feinheiten in der Verteilung der Primzahlen bis $\sqrt{x}$ gibt, welche die Primzahlen in der Umgebung von $x$ beeinflussen, und die in unserem vereinfachten Modell, das von der Unabhängigkeit der Teilbarkeit durch verschiedene Primzahlen ausgeht, nicht berücksichtigt werden. Anders ausgedrückt ist das Sieb des Eratosthenes, bei dem nur durch die Primzahlen bis $\sqrt{x}$ gesiebt wird, „speziell“ in dem Sinne, dass es die Primzahlen effizienter aussiebt, als dies ein „zufälliges“ Sieb kann.

Ein entsprechendes Programm in DERIVE, zur numerischen Auswertung der Formel (2.1) könnte etwa so aussehen:

```
wprim(n) :=
  PRODUCT(1 - 1/p, p, SELECT(PRIME(d), d, 1, FLOOR(SQRT(n))))
```

Damit sind wir in der Lage, Tabelle 2.1 anzufertigen. Mit ihrer Hilfe kann versucht werden, die obige Frage nach der Kardinalität von $\mathbb{P}$ zu beantworten.

Scheinbar sinkt mit wachsendem $n$ die Wahrscheinlichkeit, dass eine Zahl dieser Größenordnung prim ist. Bei genauerer Betrachtung des Produktes (2.1) ist dies auch nicht weiter verwunderlich, bildet man doch das Produkt

| $n$ | $\mathcal{W}(n \in \mathbb{P})$ | Rechenzeit |
|---|---|---|
| $10^1$ | 0.3333333333 | 0.00s |
| $10^2$ | 0.2285714285 | 0.00s |
| $10^3$ | 0.1528521513 | 0.00s |
| $10^4$ | 0.1203172904 | 0.00s |
| $10^5$ | 0.09651938696 | 0.01s |
| $10^6$ | 0.08096526350 | 0.02s |
| $10^{10}$ | 0.04875291783 | 2.59s |
| $10^{12}$ | 0.04063820999 | 30.6s |

Tabelle 2.1: Die Wahrscheinlichkeiten, dass eine Zahl der Größe $n$ prim ist.

über Zahlen, die allesamt echt kleiner 1 sind. Je größer man $n$ wählt, umso mehr Faktoren kommen im Produkt dazu, also umso kleiner wird schließlich das Ergebnis.

Demnach könnte man annehmen, dass die Primzahlen für wachsendes $n$ „ausdünnen“ und es somit nur endlich viele Primzahlen gibt:

$$\exists N \in \mathbb{N} : |\mathbb{P}| = N. \tag{2.4}$$

Tatsächlich aber täuscht diese Beobachtung und es gilt der folgende

**Satz 2.1.2 (Euklid)** *Es gibt unendlich viele Primzahlen.*

Für diesen Satz existieren zahlreiche Beweise, ein erster ist uns von Euklid (um 300 vor Chr.) überliefert. Dieser wird oft als typisches Beispiel für einen indirekten Beweis angeführt, und ist somit weit verbreitet.

In Folge dessen werden nachstehend zwei weitere gebracht. Eine Fülle zusätzlicher Beweise, sowie der von Euklid, können im Buch [Rib96] oder bei [15] nachgelesen werden. Darüber hinaus werden im Laufe dieser Arbeit einige Resultate geliefert, aus denen Satz 2.1.2 ebenfalls folgt, was an der entsprechenden Stelle angemerkt wird.

Der erste der beiden oben angesprochenen Beweise geht auf Polya (1887-1985) zurück. Er stützt sich auf folgende Eigenschaft der Fermat'schen Zahlen:

**Satz 2.1.3** *Je zwei verschiedene Fermat'sche Zahlen sind teilerfremd.*

*Beweis:* Seien $F_n$ und $F_{n+k}$ mit $k > 0$ die beiden Fermat'schen Zahlen, und betrachten wir ein zunächst beliebiges $m \in \mathbb{N}^\times$ mit

$$m \mid F_n = 2^{2^n} + 1, \qquad m \mid F_{n+k} = 2^{2^{n+k}} + 1. \tag{2.5}$$

Setzen wir $x = 2^{2^n}$, dann folgt

$$\frac{F_{n+k} - 2}{F_n} = \frac{2^{2^{n+k}} - 1}{2^{2^n} + 1} = \frac{x^{2^k} - 1}{x + 1} = x^{2^k - 1} - x^{2^k - 2} + \cdots - 1; \tag{2.6}$$

also gilt $F_n \mid F_{n+k} - 2$. Somit ist

$$m \mid F_{n+k}, \qquad m \mid F_{n+k} - 2, \tag{2.7}$$

und deshalb $m \mid 2$. Da $F_n$ ungerade ist, muss $m = 1$ gelten, da aus $m \mid 2$ insbesondere $m \leq 2$ folgt. Damit ist der Satz bewiesen. □

Unter Zuhilfenahme von Satz 2.1.3 ergibt sich nunmehr:

*1. Beweis: von Satz 2.1.2*
Jede der Fermat'schen Zahlen $F_1, F_2, \ldots, F_n$ wird durch eine ungerade Primzahl geteilt, die in keiner der anderen Zahlen aufgeht; deshalb gibt es mindestens $n$ ungerade Primzahlen unterhalb von $F_n$. Somit haben wir eine unendliche Folge von teilerfremden Zahlen gefunden, und der Satz von Euklid ist bewiesen. □

Der zweite Beweis läuft - so wie der Euklidische - indirekt ab, und liefert uns ein Zwischenresultat, das wir im Anschluss gleich wieder verwenden werden:

*2. Beweis: von Satz 2.1.2*
Wir nehmen an, es gäbe nur endlich viele Primzahlen, nennen wir sie $p_1, \ldots, p_r$, und bilden

$$\prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)^{-1} = \prod_{i=1}^{r} \left(1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \cdots\right). \tag{2.8}$$

Da die unendlichen Reihen auf der rechten Seite alle absolut konvergieren, kann man sie gliedweise ausmultiplizieren, und die entstehende Reihe muss wieder konvergieren:

$$\prod_{i=1}^{r} \left(1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \cdots\right) = \sum_{n \ p_r - glatt} \frac{1}{n}. \tag{2.9}$$

Da sich aber nach dem Fundamentalsatz der Zahlentheorie 1.1.2 jede Zahl $n$ als Produkt von Primzahlpotenzen schreiben lässt, müsste rechts im Nenner jede Zahl $n$ auftreten, da wir zu Beginn des Beweises angenommen haben, dass $p_1, \ldots, p_r$ schon alle Primzahlen sind. Die auf der rechten Seite von (2.9) stehende Reihe müsste also gleich der Reihe $\sum_{n=1}^{\infty} \frac{1}{n}$ sein, von der jedoch bekannt ist, dass sie divergiert. Dies ist ein Widerspruch, womit unsere Annahme widerlegt ist. □

Ganz analog zum eben abgeschlossenen Beweis folgt auch

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = \sum_{n \ x-glatt} \frac{1}{n}. \tag{2.10}$$

Insbesondere ist

$$\sum_{n \ x-glatt} \frac{1}{n} \geq \sum_{n \leq x} \frac{1}{n} > \int_1^{[x]+1} \frac{d\xi}{\xi} > \ln x. \tag{2.11}$$

Aus (2.10) und (2.11) folgt nun durch Logarithmieren ($x > 1$)

$$\sum_{p \leq x} \ln \left(1 - \frac{1}{p}\right)^{-1} > \ln \ln x \tag{2.12}$$

Nun gilt mit Lemma 1.2.2

$$\begin{aligned} \ln \left(1 - \frac{1}{p}\right)^{-1} &= -\ln \left(1 - \frac{1}{p}\right) = \frac{1}{p} + \frac{1}{2p^2} + \cdots < \\ &< \frac{1}{p} + \frac{1}{p^2} + \cdots = \frac{1}{p} + \frac{1}{p(p-1)}, \end{aligned} \tag{2.13}$$

und daher folgt aus (2.12)

$$\sum_{p \leq x} \frac{1}{p} > \ln \ln x - \sum_{p \leq x} \frac{1}{p(p-1)} > \ln \ln x - \underbrace{\sum_{n=2}^{\infty} \frac{1}{n(n-1)}}_{=1} \tag{2.14}$$

Somit folgt nunmehr, wenn wir dieses Resultat für $x \to \infty$ betrachten, der folgende Satz von Euler:

**Satz 2.1.4 (Euler)** *Die Reihe*

$$\sum_{p \in \mathbb{P}} \frac{1}{p} \tag{2.15}$$

*ist divergent.*

**Folgerung 2.1.5** *Natürlich folgt auch aus diesem Satz unmittelbar, dass es unendlich viele Primzahlen gibt, da eine endliche Anzahl die Konvergenz der Summe über die Reziprokwerte bedeuten würde.*

Eine Reihe weiterer Beweise von Satz 2.1.4 findet sich etwa in [VE80].

### 2.1.2 Die Verteilung der Primzahlen

Nachdem wir die Anzahl der Primzahlen untersucht haben, können wir uns der Frage widmen, wie regelmäßig Primzahlen in den natürlichen Zahlen auftreten. In der Tabelle 2.2 ist die Anzahl der Primzahlen in den Intervallen $[1, n]$ aufgelistet.

| $n$ | $\lvert\{p \in \mathbb{P} \mid 1 \leq p \leq n\}\rvert$ |
|---|---|
| $10^1$ | 4 |
| $10^2$ | 25 |
| $10^3$ | 168 |
| $10^4$ | 1.229 |
| $10^5$ | 9.592 |
| $10^6$ | 78.498 |
| $10^7$ | 664.579 |
| $10^8$ | 5.761.455 |
| $10^9$ | 50.847.534 |
| $10^{10}$ | 455.052.512 |

Tabelle 2.2: Die Anzahl der Primzahlen $p$ mit $1 \leq p \leq n$.

Diese Tabelle lässt vermuten, dass die Primzahlen immer seltener werden, eine Beobachtung die uns auch schon zu der Vermutung veranlasst hat, dass es nur endlich viele Primzahlen gibt. Tatsächlich kann man zu jeder beliebigen Schranke $s$ zwei aufeinanderfolgende Primzahlen $p_r$ und $p_{r+1}$ finden, die sich um mindestens $s$ unterscheiden:

**Satz 2.1.6** *Es gibt in der Folge der natürlichen Zahlen beliebig große Lücken, die keine Primzahlen enthalten, d.h. beliebig lange Ketten aufeinanderfolgender nicht primer Zahlen.*

*Beweis:* Sei $n \in \mathbb{N}^{\times}$ eine beliebige natürliche Zahl, dann sind die Zahlen

$$(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + n, (n+1)! + (n+1) \qquad (2.16)$$

gerade $n$ aufeinanderfolgende, zusammengesetzte Zahlen, denn:
Sei etwa $g = (n+1)! + k$ mit $2 \leq k \leq n+1$, dann gilt $k \mid k$, $k \mid (n+1)!$, also $k \mid g$, wobei $k \neq 1$ $(2 \leq k)$ und $k \neq g$ $(g = (n+1)! + k > k)$. □

**Bemerkung 2.1.7** *Diese Lücken können natürlich schon früher eintreten, etwa für* $n = 4$ *bildet die Zahlenfolge* $24, 25, 26, 27$ *schon eine Lücke, wie gewünscht, wobei* $24$ *wesentlich kleiner ist, als* $(4+1)! + 2 = 5! + 2 = 122$.

Das Studium der Primzahlverteilung konzentriert sich in erster Linie auf die Untersuchung der Primzahlfunktion $\pi(x)$, welche die Anzahl der Primzahlen $p \leq x$ angibt. Es ist dies eine der wichtigsten zahlentheoretischen Funktionen, ihre Werte zu berechnen ist allerdings eine extrem komplizierte und arbeitsintensive Aufgabe.

Obwohl es eine Fülle an unterschiedlichen Berechnungsmethoden gibt, gelangt man nach wie vor schnell an die Grenzen des derzeit Machbaren. Der erst kürzlich verbesserte Rekord liegt nun bei

$$\pi(10^{22}) = 201.467.286.689.315.906.290 \tag{2.17}$$

Es ist keine einfache explizite Formel bekannt, die es gestattet, $\pi(x)$ schnell und genau zu berechnen, wenn $x$ vorgegeben ist. Wir werden allerdings später sehen, dass unter geeigneten Voraussetzungen doch eine einfache Darstellung existiert. Vorerst begnügen wir uns mit dem historisch gesehen ersten Ergebnis in dieser Richtung, dem folgenden

**Satz 2.1.8 (Tschebyschew)**

$$0.89\frac{x}{\ln(x)} \leq \pi(x) \leq 1.11\frac{x}{\ln(x)} \tag{2.18}$$

Er gilt als Vorstufe zum berühmten Primzahlsatz

**Satz 2.1.9 (Primzahlsatz)**

$$\lim_{x\to\infty} \frac{\pi(x)\ln x}{x} = 1 \qquad \textit{oder} \qquad \pi(x) \sim \frac{x}{\ln x}. \tag{2.19}$$

Wir werden später noch ausführlich auf die Funktion $\pi(x)$ und die damit verbundenen Fragen zurückkommen (siehe Abschnitt 3.4, bzw. [Rie94]).

### 2.1.3 Primzahlerzeugende Funktionen

Die beliebig großen Lücken aus dem vorigen Abschnitt machen das Auffinden von Primzahlen nicht gerade einfacher. Nun kann man sich aber die Frage nach einer Funktion stellen, die ausschließlich Primzahlen liefert - das würde die Generierung von beliebig vielen Primzahlen ermöglichen. Der nächste Satz bringt in diesem Zusammenhang eine Enttäuschung mit sich:

**Satz 2.1.10** *Es gibt kein ganzzahliges Polynom $f(x) \in \mathbb{Z}[x]$ der Gestalt*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, n \geq 1, a_n \neq 0 \tag{2.20}$$

*welches für jedes $x = 1, 2, 3, \ldots$ prim ist.*

*Beweis:* Angenommen, es gäbe so ein Polynom; nennen wir es $f(x)$. Dann gilt für ein hinreichend großes $n_0$ sicherlich $|f(n_0)| > 1$. Wir nehmen nun eine Primzahl $p$ mit $p \mid f(n_0)$, und bilden

$$f(n_0 + kp) = f(n_0) + kpf_1(n_0, p, k). \tag{2.21}$$

$f_1(n_0, p, k)$ ist dabei wieder ganz, und die Zahlen (2.21) sind für $k = 1, 2, 3, \ldots$ sämtlich durch $p$ teilbar und für genügend großes $k$ jedenfalls nicht prim. Denn für genügend großes $k$ ist $|f(n_0 + kp)| > p$ und enthält entweder $p$ in mindestens zweiter Potenz oder außer $p$ noch andere Primzahlen. □

Es gibt also offensichtlich kein ganzzahliges Polynom $f(x) \in \mathbb{Z}[x]$, welches nur Primzahlwerte annimmt. Umso erstaunlicher sind daher die folgenden beiden Resultate:

Dem Mathematiker Mills ist es nämlich gelungen, eine zahlentheoretische Funktion zu konstruieren, die nur Primzahlwerte annimmt. Er bewies die Existenz einer irrationalen Zahl $A$ mit der Eigenschaft, dass $[A^{3^x}]$ für $x = 1, 2, 3, \ldots$ stets eine Primzahl ist (siehe [Mil47], bzw. [Dud69]). Dieses erstaunliche Resultat hat jedoch lediglich theoretische Bedeutung, da man nur sehr wenige Stellen von $A$ explizit kennt, so dass sich kaum Primzahlen wirklich berechnen lassen.

Auf den folgenden Satz trifft diese Einschränkung leider auch zu. Für seinen Beweis benötigen wir überdies ein Resultat, welches wir erst später zeigen werden.

**Satz 2.1.11 (Wright)** *Es gibt eine reelle Zahl $\alpha = \alpha_0$ mit der Eigenschaft, dass sämtliche mit der Rekursionsformel $\alpha_{n+1} = 2^{\alpha_n}$ bestimmten Zahlen $[2^{\alpha_0}]$, $[2^{\alpha_1}]$, $[2^{\alpha_2}], \ldots$ Primzahlen sind.*

*Beweis:* Nach 2.3.1 existiert zwischen $n$ und $2n$ mindestens eine Primzahl $p$, sodass wir also eine Folge von Primzahlen $P_1, P_2, \ldots$ so auswählen können, dass:

$$2^{P_n} < P_{n+1} < P_{n+1} + 1 < 2^{P_n+1}. \qquad (n = 1, 2, \ldots) \tag{2.22}$$

Mit $\operatorname{ld} x$ bezeichnen wir den Logarithmus von $x$ zur Basis 2 und $\operatorname{ld}^{(n)} x$ bedeute den $n$-fachen Logarithmus von $x$ zur Basis $2 : \operatorname{ld}\operatorname{ld}\ldots\operatorname{ld} x$. Aus (2.22) erhält man durch Logarithmieren

$$\operatorname{ld}^{(n)} P_n < \operatorname{ld}^{(n+1)} P_{n+1} < \operatorname{ld}^{(n+1)}(P_{n+1} + 1) < \operatorname{ld}^{(n)}(P_n + 1). \tag{2.23}$$

Setzt man

$$\beta_n := \operatorname{ld}^{(n)} P_n, \gamma_n := \operatorname{ld}^{(n)}(P_n + 1), \tag{2.24}$$

so ist

$$\beta_n < \beta_{n+1} < \gamma_{n+1} < \gamma_n. \qquad (n = 1, 2, 3, \ldots) \tag{2.25}$$

Die hieraus folgende Kette von Ungleichungen

$$\beta_1 < \beta_2 < \beta_3 < \cdots < \beta_n < \gamma_n < \gamma_{n-1} < \cdots < \gamma_2 < \gamma_1 \tag{2.26}$$

definiert für $n \to \infty$ offensichtlich als gemeinsemen Grenzwert der $\beta_n$ und $\gamma_n$ eine Zahl $\alpha$, wobei $\beta_n < \alpha < \gamma_n$ für alle $n$ gilt. Durch Zurückgehen von den Logarithmen auf die Numeri erhalten wir

$$\operatorname{ld}^{(n-1)} P_n < 2^{\alpha} = \alpha_1 < \operatorname{ld}^{(n-1)}(P_n + 1), \tag{2.27}$$

$$\operatorname{ld}^{(n-2)} P_n < 2^{\alpha_1} = \alpha_2 < \operatorname{ld}^{(n-2)}(P_n + 1), \tag{2.28}$$

$$\vdots$$

$$P_n < 2^{\alpha_{n-1}} = \alpha_n < P_n + 1, \tag{2.29}$$

oder $P_n = [\alpha_n]$, was zu beweisen war. □

**Bemerkung 2.1.12** *In der in diesem Beweis konstruierten Primzahlenfolge $P_n, P_{n+1}, \ldots$ bedeuten die Indizes nicht, dass $P_{n+1}$ die nächstgrößere Primzahl auf $P_n$ sein muss. Setzt man also z. B. $P_1 := 3$, dann erfüllt $P_2 := 13$ die im Beweis geforderte Eigenschaft. Ein Beispiel ist etwa in [Tro53] zu finden.*

Bei der Frage nach einer Funktion, die nur Primzahlen liefert, ist man also praktisch gescheitert. Die Vermutung Fermat's 2.2.4 hätte, wenn sie richtig gewesen wäre, auf diese Frage Antwort gegeben. Tatsächlich müssen wir sie an dieser Stelle aber schuldig bleiben.

Man könnte die Forderungen mäßigen und nur nach einer Funktion fragen, die wenigstens unendlich viele Primzahlen unter ihren Funktionswerten besitzt. Nach dem Satz 2.1.2 würde die identische Funktion

$$id : \mathbb{N} \to \mathbb{N}, id(n) = n \tag{2.30}$$

dies erfüllen. Abgesehen von trivialen Lösungen ist aber der Satz von Dirichlet 4.2.2 die einzige, die bekannt ist.

## 2.2 Primzahlen spezieller Bauart

Im Folgenden betrachten wir Zahlen von besonderer Bauart, welche sich oft durch außergewöhnliche Eleganz oder große praktische Relevanz auszeichnen. Bei diesen Zahlenfolgen stellen wir uns die Frage, welche Elemente daraus Primzahlen sind, und welche nicht. Ist es möglich, die Anzahl der primen Zahlen aus den einzelnen Folgen zu bestimmen?

Wie sieht es zum Beispiel mit Zahlen der Bauart $n^2+1$ aus? Gibt es unendlich viele Primzahlen der Form $n^2 + 1$? Man kann keine eindeutige Antwort darauf geben, aber schon im Jahre 1922 haben Hardy und Littlewood folgende Vermutung ausgesprochen:

**Vermutung 2.2.1 („Conjecture E“)** *Es gibt unendlich viele Primzahlen der Form $m^2 + 1$. Die Anzahl $P(n)$ solcher primen Zahlen kleiner als $n$ ist asymptotisch gleich*

$$P(n) \sim C\frac{\sqrt{n}}{\log n}, \tag{2.31}$$

*wobei gilt*

$$C = \prod_{p\in\mathbb{P},p=3}^{\infty}\left(1 - \frac{\left(\frac{-1}{p}\right)}{p-1}\right) = \prod_{p\in\mathbb{P},p=3}^{\infty}\left(1 - \frac{(-1)^{\frac{p-1}{2}}}{p-1}\right) \approx 1.3727. \tag{2.32}$$

Es folgten ähnliche Vermutungen zu allgemeiner gehaltenen Ausdrücken, die sich lediglich in der Konstanten $C$ unterscheiden. Sierpiński hat folgendes Resultat gezeigt:

**Lemma 2.2.2** *Für jedes beliebige $k \in \mathbb{N}$ gibt es ein positives $b$, sodass es mehr als $k$ Primzahlen der Form $a^2 + b$ gibt.*

Iwaniec kam mit seiner Aussage noch am nächsten zur ursprünglichen Vermutung. Er konnte nämlich zeigen:

**Satz 2.2.3** *Es gibt unendlich viele natürliche Zahlen $n$, für die $n^2+1$ das Produkt von höchstens 2 Primzahlen ist.*

Ein weiteres Beispiel bilden die soganannten „Repunits“, das sind Zahlen der Bauart

$$Rn := \frac{10^n - 1}{9} = \underbrace{11\ldots1}_{n} \tag{2.33}$$

Die erste Primzahl entsteht für $n = 2 : 11$, weiters für n=19,23,317,1.031. Man kann leicht einsehen, dass $n$ selber eine Primzahl sein muss, wenn $Rn$ eine Primzahl sein soll. Erst kürzlich hat Harvey Dubner bekannt gegeben, dass $R49.081$ (wahrscheinlich) prim ist (siehe [Dub]).

Die Frage nach der Anzahl der primen $Rn$ ist jedoch noch ein offenes Problem. Dubner betrachtet weiters auch verallgemeinerte Repunits der Form

$$M = \frac{b^n - 1}{b - 1} \tag{2.34}$$

($b$ beliebig). Er konnte dazu für $b < 99$ eine Liste möglicher Primzahlen angeben (siehe [Dub93]).

Im Folgenden werden einige „Primzahlarten“ genauer betrachtet. Es gibt jedoch eine Fülle weiterer Beispiele (etwa sogenannte „Cullen Primzahlen“ $C_n := n \cdot 2^n + 1$ bzw. $W_n := n \cdot 2^n - 1$, siehe [Kel95], oder Primzahlen der Bauart $n! \pm 1$, und viele mehr), auf die hier nicht eingegangen wird.

### 2.2.1 Fermat'sche Primzahlen

Pierre de Fermat ist spätestens seit 1994, als Andrew Wiles gemeinsam mit Richard Taylor nach jahrelanger intensiver Arbeit der vollständige Beweis des Großen Fermat'schen Satzes (Satz 1) gelang, einer breiten Öffentlichkeit bekannt. Auch die nach ihm benannte Zahlenfolge gehört mit den Mersenne'schen Primzahlen zu den bekannteren „Primzahlen“ spezieller Bauart.

Ihre Wichtigkeit ist unbestritten, hatte doch Gauss in seinen jungen Jahren bereits gezeigt, dass ein regelmäßiges $n-$Eck dann und nur dann mit Zirkel und Lineal konstruierbar ist, wenn es von der Form

$$2^n p_1 \cdots p_n \tag{2.35}$$

ist, wobei die $p_i$ Fermat'sche Primzahlen sind.

Außerdem wird $F_4 = 65.537$ gerne in der Kryptologie beim RSA-Verfahren verwendet. Dabei müssen Potenzen der Form $a^e$ mod $N$ bestimmt werden, wobei die Wahl $e = F_n$ von Vorteil ist. Der Grund hierfür liegt in der besonders einfachen Möglichkeit, diese Pontenz auszurechnen, wenn $e$ die Form $2^k + 1$ besitzt, zumal $e$ in binärer Schreibweise dann nur aus 2 Einser besteht.

Pierre de Fermat hat im Jahre 1637 folgende Vermutung geäußert:

**Vermutung 2.2.4 (Fermat)** *Alle Zahlen der Form $2^{2^n} + 1$ mit $n \in \mathbb{N}$ sind Primzahlen.*

Untermauert hat er dies bekanntlich mit der Tatsache, dass $2^{2^0} + 1 = 3 \in \mathbb{P}$, $2^{2^1} + 1 = 5 \in \mathbb{P}, 2^{2^2} + 1 = 17 \in \mathbb{P}, 2^{2^3} + 1 = 257 \in \mathbb{P}$ und schließlich $2^{2^4} + 1 = 65.537 \in \mathbb{P}$ gilt. Mit $F_5 = 2^{2^5} + 1$ stieß Fermat an die Grenzen der damaligen Möglichkeiten, eine gegebene Zahl auf ihre Primalität zu untersuchen.

Man kann leicht zeigen, dass, wenn eine Primzahl von der Form $2^m + 1$ existieren soll, $m = 2^k$ für ein $k \in \mathbb{N}$ gelten muss:

**Satz 2.2.5** *Ist $p = 2^m + 1$ eine ungerade Primzahl, dann gilt $m = 2^k$ für ein $k \in \mathbb{N}$.*

*Beweis:* Angenommen, $p = 2^m + 1$ sei eine ungerade Primzahl und $m$ habe einen ungeraden Faktor $j$, also sei $m = jl$, dann betrachtet man folgenden Quotienten

$$\frac{2^m + 1}{2^l + 1} = \frac{2^{jl} + 1}{2^l + 1}, \tag{2.36}$$

und sieht, dass das Ergebnis wiederum eine ganze Zahl ist, denn es gilt

$$\frac{2^{jl} + 1}{2^l + 1} = 2^{(j-1)l} - 2^{(j-2)l} + \cdots + 1 = \sum_{n=1}^{j} (-1)^{n+1} 2^{(j-n)l}. \tag{2.37}$$

Es besitzt also insbesondere $2^m + 1$ einen echten Teiler, sodass $2^m + 1$ keine Primzahl sein kann, was im Widerspruch zur Annahme steht. □

Man kann auch erstaunliche Aussagen über die Gestalt von Teilern Fermat'scher Zahlen machen:

**Satz 2.2.6 (Euler)** *Sei $n \geq 2$, dann hat jeder Primfaktor $p$ von $F_n = 2^{2^n} + 1$ die Gestalt $k(2^{n+2}) + 1$.*

Wir wollen uns aber jetzt mit der Frage nach der Anzahl der Fermat'schen Primzahlen beschäftigen. Auch hier zunächst eine heuristische Überlegung:

Wie wir wissen, ist die Wahrscheinlichkeit, dass eine Zahl der Größenordnung $n$ prim ist, etwa gleich $\frac{1}{\ln n}$. Somit ergibt sich für den Erwartungswert der Anzahl der Fermat'schen Primzahlen folgender Ausdruck:

$$\begin{aligned}\sum_{n=0}^{\infty} \frac{1}{\ln\left(2^{2^n}+1\right)} &\approx \sum_{n=0}^{\infty} \frac{1}{\ln\left(2^{2^n}\right)} = \sum_{n=0}^{\infty} \frac{1}{2^n \ln(2)} \\ &= \frac{1}{\ln(2)} \underbrace{\sum_{n=0}^{\infty} \frac{1}{2^n}}_{=2} = \frac{2}{\ln(2)} \approx 2.885390081. \end{aligned} \tag{2.38}$$

Man kann also erwarten, dass es nur endlich viele Fermat'sche Primzahlen gibt, insbesondere dass keine zusätzlichen zu $F_0, \ldots, F_4$ gefunden werden. Wir könnten uns somit auf unsere Heuristik berufen und folgende Vermutung äußern:

**Vermutung 2.2.7** *Die Anzahl der Fermat'schen Primzahlen $F_n = 2^{2^n}+1$ ist endlich.*

Es sei aber darauf hingewiesen, dass wir weit entfernt von einem Beweis sind. Tatsächlich wachsen die Fermat'schen Zahlen für steigendes $n$ derart stark an, dass man lange Zeit bereits bei $F_{24}$ nicht wusste, ob sie prim ist oder zusammengesetzt. Mittlerweile ist die kleinste Zahl, die man nicht einordnen kann, $F_{33}$ (Stand: Februar 2002).

In der Tabelle 2.3 sind die Untersuchungsergebnisse zu den ersten 33 Fermat'schen Zahlen aufgelistet. Für weitere Informationen siehe [BCDVH00], [CW80], [You98], bzw. [18]. Wenn eine Zahl $F_n$ nicht komplett faktorisiert ist, dann wollen wir sie kurz so schreiben

$$F_n = \prod_i p_i \cdot C. \tag{2.39}$$

Der Unterschied zwischen dem Status „teilweise faktorisiert“ und „Teiler bekannt“ liegt nun in der Information über $C$. Bei letzterem kann man über $C$ noch nichts aussagen, bei „teilweise faktorisiert“ weiß man, dass $C$ zusammengesetzt ist, kennt jedoch noch keinen Teiler von $C$.

| n | Status | $\#d$ | Jahr | Entdecker | Lit. |
|---|---|---|---|---|---|
| 0 | prim | 1 | 1637 | Fermat | |
| 1 | prim | 1 | 1637 | Fermat | |
| 2 | prim | 1 | 1637 | Fermat | |
| 3 | prim | 1 | 1637 | Fermat | |
| 4 | prim | 1 | 1637 | Fermat | |
| 5 | komplett faktorisiert | 2 | 1732 | Euler | |
| 6 | komplett faktorisiert | 2 | 1880 | Landry | [Wil93] |
| 7 | komplett faktorisiert | 2 | 1970 | Morrison & Brillhart | |
| 8 | komplett faktorisiert | 2 | 1980 | Brent & Pollard | [BP81] |
| 9 | komplett faktorisiert | 3 | 1990 | Lenstra et al. | |
| 10 | komplett faktorisiert | 4 | 1995 | Brent et al. | [Bre99] |
| 11 | komplett faktorisiert | 5 | 1988 | Brent et al. | |
| 12 | teilweise faktorisiert | 5 | 1986 | Baillie et al. | |
| 13 | teilweise faktorisiert | 4 | 1995 | Brent et al. | [BCDVH00] |
| 14 | zusammengesetzt | 0 | 1963 | Selfridge & Hurwitz | [SH64] |
| 15 | teilweise faktorisiert | 3 | 1997 | Crandall et al. | [BCDVH00] |
| 16 | teilweise faktorisiert | 2 | 1996 | Crandall et al. | [BCDVH00] |
| 17 | teilweise faktorisiert | 1 | 1978 | Gostin | |
| 18 | teilweise faktorisiert | 2 | 1999 | Crandall et al. | |
| 19 | teilweise faktorisiert | 2 | 1963 | Wrathall et al. | |
| 20 | zusammengesetzt | 0 | 1987 | Buell & Young | [YB88] |
| 21 | teilweise faktorisiert | 1 | 1963 | Wrathall | |
| 22 | zusammengesetzt | 0 | 1993 | Crandall et al. | [CDNY95] |
| 23 | Teiler bekannt | 1 | 1878 | Pervushin | |
| 24 | zusammengesetzt | 0 | 1999 | Mayer et al. | [7] |
| 25 | Teiler bekannt | 3 | 1987 | McLaughlin et al. | |
| 26 | Teiler bekannt | 1 | 1963 | Wrathall | |
| 27 | Teiler bekannt | 2 | 1985 | Gostin & Wrathall | |
| 28 | Teiler bekannt | 1 | 1997 | Taura | |
| 29 | Teiler bekannt | 1 | 1980 | Gostin & McLaughlin | |
| 30 | Teiler bekannt | 2 | 1963 | Wrathall | |
| 31 | Teiler bekannt | 1 | 2001 | Kruppa & Forbes | |
| 32 | Teiler bekannt | 1 | 1963 | Wrathall | |
| 33 | unbekannt | | | | |

Tabelle 2.3: Der aktuelle Stand bei der Faktorisierung der Fermat'schen Zahlen $F_n$ bis zur ersten Zahl $F_{33}$, wo man nicht weiß, ob sie zusammengesetzt ist, oder nicht. Die dritte Spalte beinhaltet die Anzahl der bekannten Teiler, das Jahr bezieht sich auf die Entdeckung des letzten Teilers, ebenso wie die aufgelisteten Namen (siehe [18]).

Gilt eine Zahl $F_n$ „nur“ als „zusammengesetzt“, so scheint daneben das Jahr und der Verfasser das dazugehörigen Beweises auf.

Die größte derzeit bewiesene zusammengesetzte Fermat'sche Zahl ist $F_{382.447}$, von der Cosgrave & Gallot im Jahre 1999 zeigen konnten, dass sie als Teiler $3 \cdot 2^{382.449}$ besitzt. Im 400. Geburtsjahr von Fermat kennt man mittlerweile 200 zusammengesetzte Fermat'sche Zahlen.

Im Jahre 1732 gelang es Euler erstmals eine Fermat'sche Zahl zu faktorisieren, indem er zeigte

$$F_5 = 2^{2^5} + 1 = 641 \cdot 6.700.417. \tag{2.40}$$

Knapp 150 Jahre später hat Landry 1880 bewiesen, dass

$$F_6 = 2^{2^6} + 1 = 274.177 \cdot 67.280.421.310.721 \tag{2.41}$$

gilt. Interessant sind wohl noch die beiden nächsten Fälle $n = 7$ und $n = 8$, für die Morehead und Western bewiesen haben, dass die dazugehörigen Fermat'schen Zahlen $F_n$ zusammengesetzt sind, ohne einen Faktor bestimmen zu können.

Fermat hätte mit seiner Vermutung eine Antwort auf die Frage, ob es eine Funktion gibt, die nur Primzahlen liefert, gegeben - wäre sie nicht falsch gewesen. Diesen „Fehler“ versucht man jetzt dadurch zu umgehen, dass man vorgeschlagen hat, die Fermat'sche Folge durch die Folge

$$2 + 1, 2^2 + 1, 2^{2^2} + 1, 2^{2^{2^2}} + 1, \ldots \tag{2.42}$$

zu ersetzen. Die ersten vier Zahlen sind Primzahlen, die fünfte aber liegt mit ihren 19.729 Stellen nach wie vor jenseits der Reichweite irgendeiner bekannten Methode der Faktorisierung. Wenn die Anzahl der Primzahlen $F_n$ endlich ist, dann ist natürlich die Anzahl der Primzahlen in dieser Folge a fortiori endlich.

Angesichts unserer Vermutung 2.2.7 erscheint auch die folgende nicht weiters verwunderlich:

**Vermutung 2.2.8** *Die Summe der Reziprokwerte über alle Fermat'schen Primzahlen konvergiert, d.h.*

$$\sum_{F_n \in \mathbb{P}} \frac{1}{F_n} = \alpha \in \mathbb{Q}. \tag{2.43}$$

Man ist sogar versucht, folgendes anzunehmen:

$$\alpha = \frac{1}{3} + \frac{1}{5} + \frac{1}{17} + \frac{1}{257} + \frac{1}{65.537} = \frac{2.560.071.829}{4.294.967.295} \approx 0.5960631718. \quad (2.44)$$

### 2.2.2 Mersenne'sche Primzahlen

Die zweite weithin bekannte Folge Zahlen spezieller Bauart bilden die nach einem französischen Mönch benannten Mersenne'schen Zahlen. Es handelt sich hierbei um Zahlen der Form

$$M_p := 2^p - 1, p \in \mathbb{P}. \quad (2.45)$$

Wie man leicht sieht, ist die Bedingung $p \in \mathbb{P}$ für die Primalität notwendig: Betrachtet man $2^m - 1$ mit $m = ab$, dann gilt:

$$2^m - 1 = 2^{ab} - 1 = \left(2^a - 1\right)\left(2^{(b-1)a} + 2^{(b-2)a} + \cdots + 2^a + 1\right), \quad (2.46)$$

sodass wir einen echten Teiler von $2^m - 1$ gefunden haben, $2^m - 1$ also nicht prim sein kann.

Leider ist diese Bedingung aber nicht hinreichend. 1640 hatte Mersenne folgende Behauptung aufgestellt:

$M_q$ mit $q \leq 257$ ist prim für $q \in \{2, 3, 5, 7, 11, 13, 17, 19, 31, 67, 127, 257\}$.

Diese in Hinblick auf die beachtliche Größe der beteilgten Zahlen beeindruckende Aussage konnte erst zu Beginn des vorigen Jahrhundertes vollständig überprüft werden, und erwies sich dabei als falsch: zum einen irrte sich Mersenne bei den Zahlen 67 und 257, zum anderen vergaß er 61, 89 und 107 in seine Liste aufzunehmen.

Es ist offensichtlich nicht einfach zu bestimmen, ob eine Mersenne'sche Zahl prim ist, oder wenn nicht, welche Teiler sie besitzt. Ein klassisches Ergebnis diesbezüglich geht auf Euler zurück, und wurde 1775 von Lagrange, und 1878 von Lucas, bewiesen (siehe etwa [Rib96]):

**Satz 2.2.9** *Sei $q \in \mathbb{P}$ und $q \equiv 3(4)$, dann teilt $2q+1$ $M_q$ dann und nur dann, wenn $2q + 1 \in \mathbb{P}$; in diesem Fall ist also $M_q$ zusammengesetzt.*

Primzahlen wie in diesem Satz, wo $p$ und $2p + 1$ prim sind, werden später noch extra behandelt (siehe Abschnitt 2.2.4).

Mit Hilfe des 2. Ergänzungssatzes 1.1.9 lässt sich zeigen:

**Satz 2.2.10** *Sei $n$ ein Teiler von $M_q$, dann gilt $n \equiv \pm 1(8)$ und $n \equiv 1(q)$.*

Es gibt auch eine Vermutung von Gillies über die Verteilung der Teiler Mersenne'scher Zahlen aus dem Jahre 1964, mit denen sich z.B. die Arbeiten [Ehr67], [Wag78] beschäftigen.

Die heutige Liste der Mersenne'schen Primzahlen umfasst 39 Stück (siehe Tabelle 2.4), darunter ist auch die derzeit größte bekannte Primzahl $2^{13.466.917} - 1$. Sie ist mit 4.053.946 Stellen die erst zweite Primzahl mit mehr als einer Million Stellen, wurde am 14. November 2001 entdeckt, und am 6. Dezember 2001 unabhängig davon verifiziert. Sie stellt die fünfte Mersenne'sche Primzahl in Folge dar, die durch GIMPS („Great Internet Mersenne Prime Search", [25]), den Einsatz tausender über das Internet verbundener Computer, berechnet und bewiesen werden konnte.

Mit wenigen Ausnahmen ist die größte bekannte Mersenne'sche Primzahl auch die größte jemals bewiesene prime Zahl allgemeiner Bauart. Das Interesse an den Mersenne'schen Primzahlen gründet in der Tatsache, dass sie eng mit den sogenannten „perfekten" Zahlen zusammenhängen. Perfekte Zahlen werden durch folgende Eigenschaft charakterisiert:

$$\sigma(n) = 2n \tag{2.47}$$

wobei $\sigma(n)$ die Teilersummenfunktion (siehe Kapitel 1) ist. Nun gibt es den folgenden berühmten Satz über den Zusammenhang von Mersenne'schen Zahlen und geraden perfekten Zahlen. Seine beiden Richtungen wurden, durch 2000 Jahre getrennt, von Euklid ($\Leftarrow$) bzw. Euler ($\Rightarrow$) bewiesen:

**Satz 2.2.11** *Eine gerade natürliche Zahl $n \in \mathbb{N}$ ist genau dann perfekt, wenn $n = 2^{p-1}M_p$ für ein $p \in \mathbb{P}$, sodass $M_p$ eine Primzahl ist.*

Diesem Resultat ist es zu verdanken, dass man bislang 39 perfekte Zahlen kennt - zweifellos wären es ohne diesen Satz deutlich weniger, hat doch die zu $2^{13.466.917} - 1$ gehörige Zahl $2^{13.466.916}(2^{13.466.917} - 1)$ stolze 8.107.892 Stellen und ist somit weit entfernt von den heutigen Möglichkeiten, eine Zahl zu faktorisieren.

**Bemerkung 2.2.12** *Tatsächlich hat man mit Satz 2.2.11 die geraden perfekten Zahlen im Griff. Ungelöst ist aber nach wie vor die Frage, ob es auch ungerade perfekte Zahlen gibt. In letzter Zeit sind vor allem zu den möglichen Teilern solcher Zahlen eine Reihe von Publikationen erschienen (siehe etwa [HJC98], [Ian99a] bzw. [Ian99b]).*

| Nr. | $q$ | Jahr | Entdecker (ev. Literatur) |
|---|---|---|---|
| 1 | 2 | – | – |
| 2 | 3 | – | – |
| 3 | 5 | – | – |
| 4 | 7 | – | – |
| 5 | 13 | 1461 | Anonym |
| 6 | 17 | 1588 | P.A. Cataldi |
| 7 | 19 | 1588 | P.A. Cataldi |
| 8 | 31 | 1750 | L. Euler |
| 9 | 61 | 1883 | I.M. Pervushin |
| 10 | 89 | 1911 | R.E. Powers |
| 11 | 107 | 1913 | E. Fauquembergue |
| 12 | 127 | 1876 | E. Lucas |
| 13 | 521 | 1952 | R.M. Robinson |
| 14 | 607 | 1952 | R.M. Robinson |
| 15 | 1.279 | 1952 | R.M. Robinson |
| 16 | 2.203 | 1952 | R.M. Robinson |
| 17 | 2.281 | 1952 | R.M. Robinson |
| 18 | 3.217 | 1957 | H. Riesel |
| 19 | 4.253 | 1961 | A. Hurwitz |
| 20 | 4.423 | 1961 | A. Hurwitz |
| 21 | 9.689 | 1963 | D.B. Gillies ([Gil64]) |
| 22 | 9.941 | 1963 | D.B. Gillies ([Gil64]) |
| 23 | 11.213 | 1963 | D.B. Gillies ([Gil64]) |
| 24 | 19.937 | 1971 | B. Tuckerman |
| 25 | 21.701 | 1978 | C.Noll & L. Nickel |
| 26 | 23.209 | 1979 | C.Noll |
| 27 | 44.497 | 1979 | H. Nelson & D. Slowinski |
| 28 | 86.243 | 1982 | D. Slowinski |
| 29 | 110.503 | 1988 | W.N. Colquitt & L. Welsh Jr. ([CWJ91]) |
| 30 | 132.049 | 1983 | D. Slowinski |
| 31 | 216.091 | 1985 | D. Slowinski |
| 32 | 756.839 | 1992 | P.Gage & D. Slowinski ([Ewi92]) |
| 33 | 859.433 | 1994 | P.Gage & D. Slowinski ([Ewi94]) |
| 34 | 1.257.787 | 1996 | P.Gage & D. Slowinski |
| 35 | 1.398.269 | 1996 | J. Armengaud & G. Woltman |
| 36 | 2.976.221 | 1997 | G. Spence & G.Woltman |
| 37 | 3.021.377 | 1998 | R. Clarkson, G. Woltman & S. Kurowski et al. |
| 38(?) | 6.972.593 | 1999 | N. Hajratwala, G. Woltman & S. Kurowski |
| 39(?) | 13.466.917 | 2001 | M. Cameron, G. Woltman & S. Kurowski |

Tabelle 2.4: Die 39 zur Zeit bekannten Mersenne'schen Primzahlen. Dabei weiß man nicht, ob zwischen den letzten dreien jeweils keine weitere prime Mersenne'sche Zahl liegt.

Wenden wir uns nunmehr wieder der Frage nach der Anzahl jener Primzahlen zu, die die Form $2^p - 1$ für ein $p \in \mathbb{P}$ haben: Analog zum Fall der Fermat'schen Zahlen wollen wir zunächst heuristisch an die Sache herangehen:

Wieder wird die Tatsache verwendet, dass die Wahrscheinlichkeit, dass eine Zahl der Größe $n$ prim ist, ungefähr $\frac{1}{\ln n}$ beträgt. Damit ergibt sich der Erwartungswert für die Anzahl der Mersenne'schen Zahlen:

$$\sum_{p\in\mathbb{P}} \frac{1}{\ln\left(2^p-1\right)} \approx \sum_{p\in\mathbb{P}} \frac{1}{\ln\left(2^p\right)} = \sum_{p\in\mathbb{P}} \frac{1}{p\ln(2)} = \frac{1}{\ln(2)} \sum_{p\in\mathbb{P}} \frac{1}{p} \tag{2.48}$$

wobei der letzte Ausdruck nach Satz 2.1.4 divergiert. Somit kommen wir im Fall der Mersenne'schen Zahlen zu folgender

**Vermutung 2.2.13** *Es gibt unendlich viele Mersenne'sche Zahlen $M_p = 2^p - 1$, die prim sind.*

Richard K. Guy schreibt in seinem Buch [Guy94]: „Es besteht keinerlei Zweifel, dass es unendlich viele Mersenne'sche Zahlen gibt, aber ein möglicher Beweis ist wiederum hoffnungslos weit entfernt". In diesem Zusammenhang gibt es aber auch eine Vermutung von H.W. Lenstra, Pomerance and Wagstaff:

**Vermutung 2.2.14** *Sei $M(x)$ die Anzahl der Primzahlen $p \leq x$ für die $2^p - 1$ prim ist. Dann gilt*

$$M(x) \sim e^\gamma \operatorname{ld} x \tag{2.49}$$

Wie findet man eine Mersenne'sche Primzahl, wie etwa einen Kandidaten $p$, für den $2^p - 1$ prim sein könnte? Auf diese Frage versucht eine sehr belustigende Vermutung eine Antwort zu geben:

**Vermutung 2.2.15 (Eberhart)** *Sei $q_n$ die $n$-te Primzahl, sodass $M_{q_n} = 2^{q_n} - 1$ die $n$-te Mersenne'sche Primzahl ist, dann ist $q_n \sim \left(\frac{3}{2}\right)^n$.*

**Bemerkung 2.2.16** *Nach einer Arbeit von Wagstaff sollte man Eberhart's Vermutung 2.2.15 auf*

$$\tilde{q}_n \sim \left(2^{e^{-\gamma}}\right)^n \approx (1.475761397)^n \tag{2.50}$$

*abändern, wobei $\gamma$ gleich dem Euler-Gamma (vgl. 1.1.4) ist.*

| $n$ | $p_n$ | $q_n$ | $\tilde{q}_n$ | $n$ | $p_n$ | $q_n$ | $\tilde{q}_n$ |
|---|---|---|---|---|---|---|---|
| 1 | 2 | 2 | 1 | 21 | 9.689 | 4.988 | 3.543 |
| 2 | 3 | 2 | 2 | 22 | 9.941 | 7.482 | 5.228 |
| 3 | 5 | 3 | 3 | 23 | 11.213 | 11.223 | 7.716 |
| 4 | 7 | 5 | 5 | 24 | 19.937 | 16.834 | 11.386 |
| 5 | 13 | 8 | 7 | 25 | 21.701 | 25.251 | 16.804 |
| 6 | 17 | 11 | 10 | 26 | 23.209 | 37.877 | 24.798 |
| 7 | 19 | 17 | 15 | 27 | 44.497 | 56.815 | 36.596 |
| 8 | 31 | 26 | 22 | 28 | 86.243 | 85.223 | 54.007 |
| 9 | 61 | 38 | 33 | 29 | 110.503 | 127.834 | 79.702 |
| 10 | 89 | 58 | 49 | 30 | 132.049 | 191.751 | 117.621 |
| 11 | 107 | 86 | 72 | 31 | 216.091 | 287.627 | 173.580 |
| 12 | 127 | 130 | 107 | 32 | 756.839 | 431.440 | 256.163 |
| 13 | 521 | 195 | 157 | 33 | 859.433 | 647.160 | 378.036 |
| 14 | 607 | 292 | 232 | 34 | 1.257.787 | 970.740 | 557.890 |
| 15 | 1.279 | 438 | 343 | 35 | 1.398.269 | 1.456.110 | 823.313 |
| 16 | 2.203 | 657 | 506 | 36 | 2.976.221 | 2.184.164 | 1.215.014 |
| 17 | 2.281 | 985 | 747 | 37 | 3.021.377 | 3.276.247 | 1.793.071 |
| 18 | 3.217 | 1.478 | 1.102 | 38 | 6.972.593(?) | 4.914.369 | 2.646.144 |
| 19 | 4.253 | 2.217 | 1.627 | 39 | 13.466.917(?) | 7.371.554 | 3.905.077 |
| 20 | 4.423 | 3.325 | 2.401 | 40 | (?) | 11.057.332 | 5.762.963 |

Tabelle 2.5: Die 39 Indizes zu den zur Zeit bekannten Mersenne'schen Primzahlen sowie die Konstanten aus der Vermutung von Eberhart und der abgewandelten Form nach Wagstaff.

Es spricht tasächlich einiges dafür, dass die abgewandelte Form der Eberhart'schen Vermutung der ursprünglichen vorzuziehen ist (siehe in diesem Zusammenhang auch Tabelle 2.5).

Folgen wir kurz noch dem Gedankengang von Manfred Schroeder (siehe [Sch83]), und gehen davon aus, dass für die zur $n$-ten Mersenne'schen Primzahl $M(n)$ gehörende Primzahl $p$ gilt

$$p \sim \left(2^{e^{-\gamma}}\right)^n. \tag{2.51}$$

Somit folgt für den Logarithmus zur Basis 2 von $p$

$$\mathrm{ld}\, p \sim n \cdot e^{-\gamma}. \tag{2.52}$$

Da $\operatorname{ld} p$ sehr nahe bei $\operatorname{ld}\operatorname{ld} M(n)$ liegt, sind obige Aussagen zu der folgenden äquivalent: Wenn wir $\operatorname{ld}\operatorname{ld} M(n)$ als Funktion von $n$ aufzeichnen, dann können wir diese Daten mittels einer Geraden, die den Anstieg $e^{-\gamma}$ besitzt, approximieren.

Dies lässt sich mit DERIVE sehr gut überprüfen. Wir beschränken uns bei diesen Untersuchungen auf die ersten 37 Mersenne'schen Primzahlen, da nicht bekannt ist, ob zwischen den letzten dreien noch weitere liegen.

Zunächst beschaffen wir uns jene 37 Primzahlen, die die ersten 37 Mersenne'schen Primzahlen erzeugen. Das kann beispielsweise so geschehen:

```
m :=  VECTOR(MERSENNE_DEGREE(n), n, 1, 37)
```

Dabei sind in der internen Variable `MERSENNE_DEGREE` alle Indizes der Mersenne'schen Primzahlen gespeichert, und wir wählen die ersten 37 davon aus. Anschließend legen wir durch diese Punkte die Regressionsgerade

```
FIT([x, ax + b], TABLE(LOG(m SUB k, 2), k, DIM(m)))
```

und erhalten folgendes Ergebnis (siehe auch Abbildung 2.1):

$$0.5641371555 \cdot x + 0.8205911725. \tag{2.53}$$

Diese Steigung ist bemerkenswert nahe bei $e^{-\gamma} \approx 0.5614594835$, womit wir in gewisser Weise die Bemerkung 2.2.16 begründet haben.

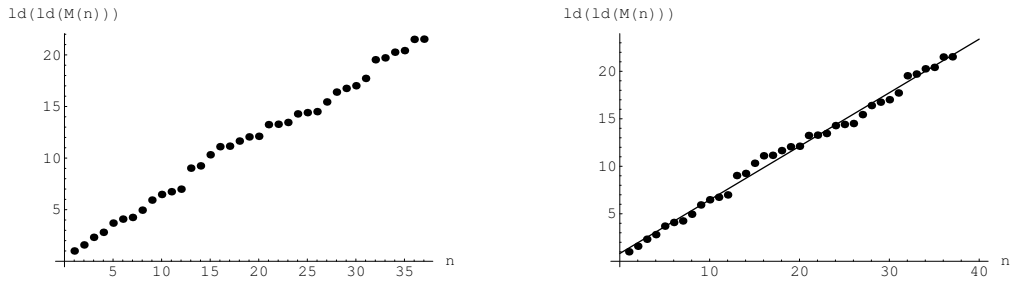


Abbildung 2.1: Die $n$-ten Mersenne'schen Primzahlen $M(n)$ als Funktion von $n$ aufgezeichnet, bzw. mit der durch diese Punkte gelegten Regressionsgeraden $0.5641371555x + 0.8205911725$.

Wenn wir nun für $x$ etwa 40 einsetzen, so gelangen wir zu der Aussage, dass bei etwa $2^{10.962.529}$ die 40. Mersenne'sche Primzahl liegen sollte. Somit könnte man also annehmen, dass tatsächlich zwischen 3.021.377 und 13.466.719 noch eine Mersenne'sche Zahl übersehen wurde, die prim ist.

Ein weiteres ungelöstes Problem ist z.B., ob für primes $p$ die Zahl $2^p - 1$ stets quadratfrei ist. Man kann zwar fast sicher annehmen, dass dem nicht so ist, doch steht ein endgültiger Beweis noch aus.

### 2.2.3 Reguläre Primzahlen

Bis zum Ende des letzten Jahrhunderts hat sich der „Große Fermat“ als hartnäckiges Problem erwiesen, bei dessen 300 Jahre lang dauernden Beweisversuchen zahlreiche nützliche Werkzeuge entdeckt und entwickelt wurden. Dazu gehören auch drei spezielle Primzahlarten.

Die erste taucht bei Kummer in Verbindung mit dem Großen Fermat im Jahre 1847 auf. In einem Brief an Liouville teilt Kummer diesem mit, dass er für Primzahlen $p$, welche 2 Bedingungen erfüllen, den Großen Fermat bewiesen hätte. Später konnte Kummer noch zeigen, dass alle Zahlen, die der ersten Bedingung genügen auch die zweite erfüllen, sodass wir heute von einer einfachen Charakterisierung der regulären Primzahlen ausgehen können:

**Definition 2.2.17** *Eine Primzahl $p$ heißt regulär dann und nur dann, wenn $p$ keinen der Zähler der Zahlen $B_2, B_4, B_6, \ldots, B_{p-3}$ teilt. Dabei werden $B_n$* Bernoulli Zahlen *genannt, die als Koeffizienten der Funktion*

$$\frac{x}{e^x - 1} = \sum_{n \geq 0} B_n \frac{x^n}{n!} \tag{2.54}$$

*definiert sind. Es gilt*

$$B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, \ldots, B_{2k} = (-1)^{k-1} \frac{2(2k)!}{(2\pi)^{2k}} \zeta(2k) \tag{2.55}$$

*wobei $\zeta$ die Riemann'sche $\zeta$-Funktion ist. (2.55) impliziert insbesondere, dass die $B_n$ sehr rasch anwachsen.*

Kummer gab alle irregulären Primzahlen kleiner als 163 an:

$$37, 59, 67, 101, 103, 131, 149, 157 \tag{2.56}$$

Diese Aussage kann innerhalb von 10 Sekunden mit einem sehr einfachen DERIVE-Programm nachgeprüft werden:

```
regular(p) :=
  SOLVE(MOD(PRODUCT(VECTOR(NUMERATOR(
      BERNOULLI(n)), n, 2, p-3, 2)), p) /= 0)
```

Das Programm `regular(p)` liefert zurück, ob eine Primzahl $p$ regulär ist oder nicht, und der Aufruf

```
SELECT(NOT regular(p),p,SELECT(PRIME(q),q,1,163))
```

liefert schließlich nach 10.2 Sekunden die Verifizierung der 8 nach Kummer irregulären Zahlen kleiner als 167.

Von den 78.498 Primzahlen kleiner als $10^6$ sind 47.627 regulär, im Einklang mit ihrer erwarteten Dichte von $e^{-\frac{1}{2}}$. Es konnte jedoch noch nicht bewiesen werden, dass es unendlich viele davon gibt. Andererseits überraschte Jensen im Jahre 1915 mit einem ziemlich einfachen Beweis, dass es unendlich viele irreguläre Primzahlen gibt.

Zur Verteilung irregulärer Primzahlen sei hier z.B. auf [Joh75], [Wag78] oder [BCS92] verwiesen.

### 2.2.4 Sophie Germain Primzahlen

Dies sind die zweiten Primzahlen spezieller Form, die in der Geschichte der Beweisversuche des Großen Fermat's auftreten. Wir haben sie auch schon im Kapitel über Mersenne'sche Primzahlen kennengelernt, wo sie in einem Kriterium nach Euler über die Teiler von Mersenne'schen Zahlen auftreten.

**Definition 2.2.18** *Sei $p$ eine Primzahl, und darüberhinaus auch $2p+1 \in \mathbb{P}$. Dann heißt $p$ eine* Sophie Germain Primzahl.

Ein Beispiel für eine große Sophie Germain Primzahl ist etwa

$$p = 18.458.709 \cdot 2^{32.611} - 1, \tag{2.57}$$

womit also $M_p$ als zusammengesetzt entlarvt ist, trotz der gewaltigen Größenordnung von $10^{10^4}$ dezimalen Stellen.

Doch zurück zum Großen Fermat. Diese Zahlen werden nach Sophie Germain benannt, weil sie folgenden Satz bewiesen hat:

**Satz 2.2.19** *Ist $p$ eine Sophie Germain Primzahl, dann gibt es keine ganzzahligen $x, y, z$, alle ungleich der Null, und keine Vielfachen von $p$, sodass $x^p + y^p = z^p$ erfüllt wird.*

Sollte jemand weiter in die Materie rund um diese Primzahlen in Verbindung mit dem Großen Fermat einsteigen, so sei er hier auf das Buch [Rib79] verwiesen.

Wieder ist nicht bekannt, ob es unendlich viele Primzahlen dieser Bauart gibt. Aber wir können uns mit sehr einfachen Mitteln unter Zuhilfenahme von DERIVE einen Überblick über die Verteilung der Sophie Germain Primzahlen verschaffen.

Zunächst schreiben wir eine Routine `next_germain(n)`, die uns zu einer gegebenen Größe $n$ das nächstgrößere $p$ ausgibt, sodass $p$ und $2p+1$ prim sind. Diese könnte zum Beispiel so aussehen:

```
next_germain(n):=
  Loop
    n := NEXT_PRIME(n)
    If PRIME(2n + 1)
       RETURN n
```

Dieses Programm wird nun in der Routine `nog(n)` verwendet, um die Anzahl der Sophie Germain Primzahlen unterhalb von $n$ zu bestimmen. (Beachte: Dabei werden alle Primzahlpaare tatsächlich berechnet, das Ergebnis ist also absolut - keine Schätzung!)

```
nog(n, p_ := 1, i_ := 0):=
  Loop
    p_ := next_germain(p_)
    If p_ > n
       RETURN i_
    If PRIME(2p_ + 1)
       i_ :+ 1
```

Damit lässt sich bis zu $n = 10^7$ relativ vernünftig die Anzahl der Sophie Germain Primzahlen bestimmen (siehe Tabelle 2.6).

Weiter wurden diese Zahlen mit DERIVE nicht untersucht, denn der zu erwartende Aufwand wäre zu groß. Auch eine etwaige Zwischenspeicherung der bisher gefundenen Paare würde hier keine wesentliche Änderung bzw. Verbesserung mit sich bringen. Man kann jedoch etwa in [Dub96] weitere Beispiele solcher Primzahlen nachschlagen.

| $n$ | $nog(n)$ | $Zeit$ |
|---|---|---|
| 10 | 3 | $0.000s$ |
| 100 | 10 | $0.010s$ |
| 1.000 | 37 | $0.010s$ |
| 10.000 | 190 | $0.081s$ |
| 100.000 | 1.171 | $0.701s$ |
| 1.000.000 | 7.746 | $11.8s$ |
| 10.000.000 | 56.032 | $939.2s$ |

Tabelle 2.6: Die Anzahl der Sophie Germain Primzahlen unterhalb von $10^7$.

An dieser Stelle sei noch angemerkt, dass die Sophie Germain Primzahlen ihre Verwendung auch im Zusammenhang mit dem RSA-Verfahren finden. Für die dabei zu wählenden Primzahlen $p$ und $q$ nimmt man aus Sicherheitsgründen zumeist sogenannte „sichere Primzahlen“, das sind solche, wo nicht nur $p$ und $q$ prim sind, sondern auch $\frac{p-1}{2}$ und $\frac{q-1}{2}$. Diese „sicheren Primzahlen“ sind also von der Form $2\tilde{p}+1$, wobei $\tilde{p}$ eine Sophie Germain Primzahl ist.

### 2.2.5 Wieferich'sche Primzahlen

Die letzte Art von Primzahlen, die bei der Suche nach dem Großen Fermat auftauchten, sind die Wieferich'schen Primzahlen. Bei ihrer Definition beginnt man beim kleinen Bruder von Fermat's letztem Satz, dem kleinen Fermat:

**Satz 2.2.20 („Kleiner Fermat“)** *Ist $p$ eine Primzahl, dann erfüllt $p$ stets folgende Kongruenz:*

$$2^{p-1} \equiv 1(p) \tag{2.58}$$

Ausgehend von diesem trivialen Ergebnis, das als Start unterschiedlichster Untersuchungen dient, wandelt man (2.58) in folgender Weise um:

$$2^{p-1} \equiv 1(p^2) \tag{2.59}$$

Nun stellt sich die Frage, welche Primzahlen die Kongruenz (2.59) erfüllen. Solche Primzahlen werden schließlich Wieferich'sche Primzahlen genannt. Er war es auch, der im Jahre 1909 folgenden schwierigen Satz beweisen konnte:

**Satz 2.2.21** *Gibt es für eine Primzahl $p$ ein Trippel $(x, y, z)$ mit $p \nmid xyz$, sodass*

$$x^p + y^p = z^p \tag{2.60}$$

*erfüllt ist, dann erfüllt $p$ die Bedingung (2.59).*

Wir können diese Primzahlen aber auch über den sogenannten „Fermat-Quotienten“ einführen:

**Definition 2.2.22** *Eine Primzahl $p$ wird Wieferich'sche Primzahl genannt, wenn für den* Fermat-Quotient

$$q_p(2) := \frac{2^{p-1} - 1}{p} \tag{2.61}$$

*gilt:*

$$q_p(2) \equiv 0(p). \tag{2.62}$$

Die Wahrscheinlichkeit für das Verschwinden von $q_p(2)$ mod $p$ liegt in etwa bei $\frac{1}{p}$. Da die Summe der Reziprokwerte über alle Primzahlen divergiert (siehe Satz 2.1.4), könnte man - einer (2.48) ähnlichen Heuristik folgend - annehmen, dass es unendlich viele Wieferich'sche Primzahlen gibt:

**Vermutung 2.2.23** *Es gibt unendlich viele Wieferich'sche Primzahlen.*

In diesem Fall empfiehlt es sich jedoch, etwas weiter in die Theorie einzudringen, um herauszufinden, dass die Bedingung (2.59) von kaum einer Primzahl $p$ erfüllt wird. Interessanterweise wurden die beiden einzigen bislang bekannten Wieferich'schen Primzahlen zu Beginn des vorigen Jahrunderts, also noch lange vor dem Computerzeitalter, gefunden: 1913 entdeckte Meissner die Zahl 1.093 und 9 Jahre später stieß Beeger mit 3.511 auf die zweite derartige Primzahl.

Ein mögliches Programm zur Auffindung dieser Primzahlen in DERIVE ist wiederum sehr einfach aufgebaut:

```
next_wieferich(n) :=
  Loop
    n := NEXT_PRIME(n)
    If MOD(2^(n - 1), n^2) = 1
       RETURN n
```

Der Computer konnte im Falle dieser Zahlen nur eingesetzt werden, um die Nichtexistenz von Wieferich'schen Primzahlen zwischen 3.511 und $16 \cdot 10^{12}$ zu beweisen (siehe z.B. [CDP97]). Man weiß nicht, ob es - abgesehen von den beiden bekannten - noch weitere Primzahlen gibt, die die Kongruenz (2.59) erfüllen. (Die Richtigkeit von Vermutung 2.2.23 ist somit mehr als fraglich!) Man weiß nicht einmal, ob es unendlich viele Primzahlen gibt, die diese Bedingung nicht erfüllen.

### 2.2.6 Wilson'sche Primzahlen

Auch hier dient eine geläufige Tatsache als Ausgangspunkt. Dabei handelt es sich um das einzige bekannte Primzahlkriterium:

**Satz 2.2.24 (Wilson)** *Eine natürliche Zahl $p \in \mathbb{N}$ ist Primzahl dann und nur dann, wenn gilt*

$$(p-1)! \equiv -1(p). \tag{2.63}$$

Abermals wechselt man den Modul von $p$ zu $p^2$ aus, und definiert:

**Definition 2.2.25** *Eine Primzahl $p$, die folgende Kongruenz*

$$(p-1)! \equiv -1(p^2) \tag{2.64}$$

*erfüllt, wird Wilson'sche Primzahl genannt. Eine weiter Möglichkeit zur Definition bietet der sogenannte „*Wilson-Quotient*“*

$$w_p := \frac{(p-1)! + 1}{p}. \tag{2.65}$$

*Eine Primzahl $p$ wird genau dann Wilson'sche Primzahl genannt, wenn*

$$w_p \equiv 0(p) \tag{2.66}$$

*gilt.*

Wieder kann für die Wahrscheinlichkeit, dass der Wilson-Quotient mod $p$ verschwindet, und dass somit die Primzahl $p$ eine Wilson'sche Primzahl ist, der Einfachheit halber $\frac{1}{p}$ angenommen werden. Auch hier können wir ohne Schwierigkeiten ein Programm in DERIVE angeben, das die nächstgrößere Wilson'sche Primzahl berechnet:

```
next_wilson(n) :=
  Loop
    n := NEXT_PRIME(n)
    If MOD(((n - 1)! + 1)/n, n) = 0
       RETURN n
```

Dabei wurde offensichtlich die zweite Möglichkeit zur Definition implementiert, nämlich über den Wilson-Quotienten.

Wie schon im vorangegangenen Abschnitt, lohnt sich eine eingehendere Auseinandersetzung mit der Thematik, denn auch in diesem Fall steht man bei der tatsächlichen Berechnung bald vor unlösbaren Aufgaben. Neben $5, 13$ und $563$ ist keine weitere Wilson'sche Primzahl bis $5 \cdot 10^8$ bekannt (siehe [CDP97]). Die größte bekannte Wilson'sche Primzahl $563$ wurde 1953 von Goldberg entdeckt, und stellt eine der ersten erfolgreichen Anwendungen eines Computers in der Zahlentheorie dar.

### 2.2.7 Primorials

Als Zwischenstufe zu unseren letzten Primzahlen spezieller Bauart betrachten wir nun kurz die sogenannten „Primorials“. Sie sind wie folgt definiert:

**Definition 2.2.26** *Sei $n \in \mathbb{N}^{\times}$ eine beliebige natürliche Zahl. Dann versteht man unter dem $n$-ten* Primorial *folgende Zahl*

$$n\# := \prod_{i=1}^{n} p_i + 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdots p_n + 1. \tag{2.67}$$

Diese an sich sehr einfache Definition läßt sich auch mühelos in DERIVE folgendermaßen implementieren:

```
primorial(n):=PRODUCT(ITERATES(NEXT_PRIME(q),q,2,n-1))+1
```

Auf der Suche nach primen Primorials glaubt man sich zunächst auf sicherem Terrain zu befinden, stellt sich doch heraus, dass die ersten 5 Primorials prim sind - genau wie bei den Fermat'schen Zahlen $F_n$. Ähnlich wie bei $F_5$, also bei der 6. Fermat'schen Zahl, wird man auch bei dem 6. Primorial $6\#$ enttäuscht, gilt doch

$$6\# = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30.031 = 59 \cdot 509. \tag{2.68}$$

Aber im Gegensatz zu den $F_n$ findet man rasch auch weitere Primzahlen in der Folge der $n\#, n = 7, 8, \ldots$

Mit der nachstehenden Funktion kann man sich in beliebigen Intervallen $[m, n]$ auf die Suche nach der Anzahl der primen Primorials begeben:

```
nopp(n,m:=1):=DIM(SELECT(PRIME(q),q,VECTOR(primorial(l),l,m,n)))
```

Es stellt sich heraus, dass die ersten 5 primen Primorials die einzigen mit $n \leq 10$ sind. Aber schon mit $11\#$ haben wir die 6. Primzahl gefunden. In der Tabelle 2.7 finden sich die ersten 10 primen $n\#$, die mit DERIVE und den obigen Routinen berechnet wurden. Sie steht auch im Einklang mit älteren Arbeiten, wie z.B. [Bor72], [Tem80], [BCP82] bzw. [Kel83].

Weiter wurde mit DERIVE nicht gesucht, aber Harvey Dubner hat entdeckt, dass Primzahlen auch für $n = 457, 616$ und 643 resultieren. Darüber hinaus ist $n\#$ prim für $n = 1.391$ und $n = 1.613$, zwei Zahlen mit 4.951 bzw. 5.862 Stellen (siehe [Dub87]).

| $nopp(n)$ | $n$ | $dim(n\#)$ | $Zeit$ |
|---|---|---|---|
| 1 | 1 | 1 | $0.000s$ |
| 2 | 2 | 1 | $0.000s$ |
| 3 | 3 | 2 | $0.000s$ |
| 4 | 4 | 3 | $0.000s$ |
| 5 | 5 | 4 | $0.000s$ |
| 6 | 11 | 12 | $0.010s$ |
| 7 | 75 | 154 | $0.721s$ |
| 8 | 171 | 425 | $12.8s$ |
| 9 | 172 | 428 | $14.3s$ |
| 10 | 384 | 1.115 | $387.2s$ |

Tabelle 2.7: Die ersten 10 primen Primorials. Um die zehnte, 1.115stellige Zahl 384# zu entdecken, benötigt `nopp(n,m)` bereits 387.2 Sekunden.

Caldwell zeigte, dass neben 2.122# auch noch 23.801# und die 10.387stellige Zahl 24.029# prim sind (siehe [Cal95]).

Über die tatsächliche Anzahl der Primzahlen in der Folge der $n\#$ kann man wieder nur eine Vermutung aufstellen:

**Vermutung 2.2.27** *Es gibt unendlich viele Primorials $n\#$, die prim sind.*

### 2.2.8 Fortune'sche Zahlen

Als letzte besondere Art von Primzahlen wollen wir uns den nach dem Anthropologen Fortune benannten „Fortune'schen Zahlen" widmen. Sie sind sehr einfach in ihrer Definition, und doch bergen sie, wie sich noch herausstellen wird, eine große Überraschung in sich.

**Definition 2.2.28** *Sei $n \in \mathbb{N}$ wieder eine beliebige natürliche Zahl, und $n\#$ wie im vorigen Abschnitt definiert. Darüberhinaus bezeichne $\wp_n$ die kleinste Primzahl, die größer als $n\#$ ist. Dann nennt man Zahlen der Bauart*

$$\mathcal{F}_n = \wp_n - n\# + 1 \tag{2.69}$$

Fortune'sche Zahlen.

Mit den Routinen des vorigen Abschnittes läßt sich auch diese Art der Primzahlen rasch in DERIVE implementieren:

```
fortune(n, k_) :=
  Prog
    k_ := primorial(n)
    k_ := NEXT_PRIME(k_) - k_ + 1
```

Wenn man einige $\mathcal{F}_n$ berechnet, so sieht man sehr bald, dass die einzelnen $\mathcal{F}_n$ nicht notwendigerweise unterschiedlich sind. Im Gegenteil: es tauchen immer wieder Primzahlen $p$ auf, für die es mehrere Zahlen $n_i$ gibt, sodass $p = \mathcal{F}_{n_i}$ gilt.

Eine einfache Routine, um festzustellen, welches Element wie oft auftaucht, könnte so aussehen:

```
noel(a, i_ := 1, q_, r_, s_ := []) :=
  Prog
    a := SORT(a)
    Loop
      q_ := a SUB i_
      r_ := SELECT(n = q_, n, a)
      s_ := APPEND_COLUMNS(s_, [q_; DIM(r_)])
      i_ :+ DIM(r_)
      if i_ > DIM(a)
         RETURN s_
```

Damit läßt sich zum Beispiel feststellen, dass unter den ersten 150 $\mathcal{F}_n$ 84 Primzahlen einfach auftreten, 22 doppelt vorkommen, 6 immerhin dreimal auftauchen und eine sogar viermal. Tatsächlich gilt

$$\mathcal{F}_{52} = \mathcal{F}_{58} = \mathcal{F}_{61} = \mathcal{F}_{64} = 331. \tag{2.70}$$

Die eigentliche, bereits angekündigte Überraschung, die diesen Zahlen eigen ist, liegt aber nicht in (2.70), sondern in der Tatsache, dass noch kein zusammengesetztes $\mathcal{F}_n$ bekannt ist! In der Tat lautet die Vermutung von Fortune folgendermaßen:

**Vermutung 2.2.29 (Fortune)** *Sei $\mathcal{F}_n$ wie in (2.69) definiert, dann ist $\mathcal{F}_n$ stets prim, für alle $n \in \mathbb{N}$.*

Wir wollen uns im Folgenden diese Vermutung etwas genauer ansehen. Dazu stellen wir die $\mathcal{F}_n$ etwas anders dar, und definieren dazu

$$P_n := p_1 \cdot p_2 \cdots p_n. \tag{2.71}$$

Damit gilt:

$$\mathcal{F}_n := \wp_n - P_n. \tag{2.72}$$

Da $\wp_n$ per Definition prim ist, kann $\mathcal{F}_n$ nicht durch $p_1, p_2, \ldots, p_n$ geteilt werden. Folglich gilt $\mathcal{F}_n \geq p_{n+1}$ für alle $n \in \mathbb{N}$. Solange andererseits $\mathcal{F}_n \leq p_{n+1}^2$ gilt, muss $\mathcal{F}_n$ prim sein, zumal die kleinste zusammengesetzte, zu $P_n$ teilerfremde Zahl gleich $p_{n+1}^2$ ist. Es ist jedoch ziemlich unwahrscheinlich, dass $\mathcal{F}_n$ überhaupt so groß wird, wie im Anschluss gezeigt wird:

Zunächst werden die folgenden 3 Eigenschaften benötigt, die unmittelbar aus dem Primzahlsatz 3.2.1 folgen:

**Lemma 2.2.30** *1.* $p_n \sim n \ln n$ *für* $n \to \infty$

*2.* $\ln P_n = \sum_{i=1}^{n} \ln p_i \sim n$ *für* $n \to \infty$

*3. Der „Erwartungswert" für die Differenz* $p_{n+1} - p_n$ *ist ungefähr* $\ln n$

Angenommen, $P_n$ sei eine zufällig ausgewählte Zahl, dann würde man die nächstgrößere Primzahl bei

$$P_n + \ln P_n \sim P_n + n \tag{2.73}$$

erwarten. Wie jedoch schon gezeigt wurde, ist $\wp_n$ zumindest

$$P_n + p_{n+1} \sim P_n + n \ln n. \tag{2.74}$$

Weiters gilt $p_{n+1} \geq p_n + 2$, also

$$p_{n+1}^2 \geq p_n^2 + 4p_n + 4, \tag{2.75}$$

womit

$$P_n + p_{n+1}^2 > P_n + p_n^2 \sim P_n + n^2 \ln^2 n \tag{2.76}$$

folgt. Da der mittlere Abstand zwischen Primzahlen der Größenordnung $P_n$ etwa $\ln P_n \sim n$ ist, kann man ungefähr $n \ln^2 n$ Primzahlen im Intervall $[P_n + 1, P_n + p_{n+1}^2]$ erwarten. Nur wenn dieses Intervall frei von Primzahlen wäre, könnte die Fortune'sche Vermutung falsch sein. Tatsächlich folgt aus den obigen Überlegungen, dass für jede Primzahl $q$ aus diesem Intervall die Differenz $q - P_n$ prim ist (das kleinste dieser $q$ ist gleich $\wp_n$!).

Die Tatsache, dass man viele Primzahlen in diesen Intervallen erwartet, ist jedoch keine Garantie dafür, dass stets wenigstens eine enthalten ist. Ein

Ergebnis derart, dass für hinreichend großes $x$ stets eine Primzahl im Intervall $[x, x + \frac{1}{2}(\ln x \ln\ln x)^2]$ liegt, ist weit jenseits allem derzeit Erreichbaren - und ist vielleicht sogar „eine zu starke Aussage, um wahr zu sein“, wie Solomon Golomb in seinem Artikel „The Evidence for Fortune's Conjecture“ zu bedenken gibt (siehe [Gol81]).

Dennoch: würde diese Aussage stimmen, dann hätte auch Fortune recht, wie man durch $x = P_n + 1$ sofort sieht. Tatsächlich würde eine Vermutung von Cramer das Gewünschte leisten, sagt sie doch aus, dass sogar zwischen $x$ und $(\ln x)^2$ stets eine Primzahl ist. Dies wiederum impliziert für hinreichend großes $n$ - das bedeutet $\frac{1}{2}\ln\ln n > 1$, also $n > 1.618$ - die Fortune'sche Vermutung. Derzeit ist kein Beweis von Cramer's Vermutung in Sicht.

## 2.3 Weitere interessante Fragestellungen

Die Überschrift lässt es schon erahnen: In diesem Abschnitt werden wir wieder mit zum Teil noch unbeantworteten Fragen konfrontiert. Generell hat es den Anschein, als wäre auf dem Gebiet der Zahlentheorie, im Vergleich zu der Fülle an unbewiesenen Vermutungen, kaum ein Resultat bewiesen. In der Tat findet man sogar eigene Bücher, die nur Vermutungen und Mutmaßungen aus der Zahlentheorie zum Inhalt haben, wie etwa das Buch [Guy94], aus dem auch so manche offene Frage in dieser Arbeit stammt.

### 2.3.1 Das Bertrand'sche Postulat

Im Abschnitt über die Fortune'schen Zahlen wurde kurz die Cramer'sche Vermutung vorgestellt, wonach im Intervall $[n, \ln^2 n]$ stets eine Primzahl liegt. Wie dort ebenfalls angemerkt, ist kein Beweis dieser Aussage bekannt, weshalb sie nach wie vor als Vermutung bezeichnet wird.

Im Folgenden soll das Hauptaugenmerk auf das Intervall $(n, 2n], n \geq 1$ gerichtet werden. Dafür gibt es ein berühmtes Resultat, welches im Zuge dieser Arbeit bewiesen werden kann:

**Satz 2.3.1 (Bertrand'sches Postulat)** *Sei $n \in \mathbb{N}^{\times}$, dann gibt es stets mindestens eine Primzahl $p$ mit $n < p \leq 2n$.*

*Beweis:* Ein erster Beweis dessen geht auf Tschebyschew und das Jahr 1850 zurück. Der nachstehende Beweis, der in 5 Schritten abläuft, folgt im Wesentlichen dem Gedankengang aus [AZ01].

In einem ersten Schritt wird das Postulat für $n < 4.000$ bewiesen, wo man - einen Trick von Landau verwendend - beobachtet, dass

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1.259, 2.503, 4.001 \tag{2.77}$$

eine Folge von Primzahlen ist, wo jede kleiner als das Doppelte der vorhergehenden ist. Somit ist die Aussage für $n < 4.000$ bewiesen, und jedes Intervall $(n, 2n]$ mit $n < 4.000$ enthält eine der 14 Primzahlen.

Für den zweiten Schritt wird zunächst das folgende Lemma bewiesen:

**Lemma 2.3.2** *Sei $m \in \mathbb{N}, m \geq 1$, dann gelten die beiden Ungleichungen*

$$\prod_{m+1<p\leq 2m+1} p \leq \binom{2m+1}{m} \leq 2^{2m}. \tag{2.78}$$

*Beweis:* Die erste Ungleichung folgt unmittelbar aus der Tatsache, dass

$$\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!} \in \mathbb{N}, \tag{2.79}$$

und die Primzahlen $p$, die wir in unserem Produkt betrachten, alle im Zähler enthalten sind, jedoch nicht im Nenner. Die zweite Ungleichung hält, da

$$\binom{2m+1}{m} \qquad \text{und} \qquad \binom{2m+1}{m+1} \tag{2.80}$$

zwei gleiche Summanden in der Summe

$$\sum_{k=0}^{2m+1} \binom{2m+1}{k} = 2^{2m+1} \tag{2.81}$$

sind. □

Unter Verwendung von Lemma 2.3.2 folgt nun:

**Lemma 2.3.3** *Sei $x \in \mathbb{R}, x \geq 2$, so gilt*

$$\prod_{p\leq x} p \leq 4^{x-1} \tag{2.82}$$

*Beweis:* Zunächst gilt für die größte Primzahl $q \leq x$

$$\prod_{p\leq x} p = \prod_{p\leq q} p \qquad \text{und} \qquad 4^{q-1} \leq 4^{x-1}. \tag{2.83}$$

Somit genügt es, (2.82) für den Fall $x = q \in \mathbb{P}$ zu zeigen. Für $q = 2$ bedeutet dies „$2 \leq 4$“, sodass es genügt, mit den ungeraden Primzahlen $q = 2m + 1$ fortzufahren. Dazu spaltet man das Produkt auf, und erhält mit Hilfe von Lemma 2.3.2 und der Induktionsvoraussetzung

$$\prod_{p \leq 2m+1} p = \prod_{p \leq m+1} p \cdot \prod_{m+1 < p \leq 2m+1} p \leq 4^m \binom{2m+1}{m} \leq 4^m 2^{2m} = 4^{2m}, \tag{2.84}$$

womit das Lemma bewiesen wäre. □

Zum dritten Schritt wird ein Resultat von Legendre benötigt, das man sich sehr leicht überlegen kann:

**Satz 2.3.4 (Legendre)** *Die Zahl $n!$ enthält die Primzahl $p$ genau*

$$\sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor \tag{2.85}$$

*mal.*

Daraus kann man ableiten, dass $\binom{2n}{n}$ die Primzahl $p$ genau

$$\sum_{k \geq 1} \left( \left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right) \tag{2.86}$$

mal enthählt. Dabei ist jeder auftretende Summand höchstens Eins, da die folgende Beziehung erfüllt ist

$$\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor < \frac{2n}{p^k} - 2 \left( \frac{n}{p^k} - 1 \right) = 2, \tag{2.87}$$

und das Ergebnis darüberhinaus eine natürliche Zahl ist. Weiters verschwinden die Summanden, sobald $p^k > 2n$ gilt. Somit enthält $\binom{2n}{n}$ $p$ genau

$$\sum_{k \geq 1} \left( \left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right) \leq \max\{r | p^r \leq 2n\} \tag{2.88}$$

mal, sodass die größte Potenz von $p$, die $\binom{2n}{n}$ teilt, nicht größer als $2n$ ist. Die Primzahlen mit $p > \sqrt{2n}$ tauchen nur einmal in $\binom{2n}{n}$ auf.

Tatsächlich aber, und dies ist nach Erdös der springende Punkt, teilen Primzahlen $p$ mit $\frac{2}{3}n < p \leq n$ die Zahl $\binom{2n}{n}$ überhaupt nicht! Aus $3p > 2n$

folgt (für $n \geq 3$, also $p \geq 3$), dass $p$ und $2p$ die einzigen Vielfachen von $p$ sind, die im Zähler von $\frac{(2n)!}{n!n!}$ auftauchen, während sie durch zwei $p$-Faktoren im Nenner wieder gekürzt werden.

Für den 4. Schritt wollen wir uns zunächst noch kurz eine Abschätzung für den Binomialkoeffizienten $\binom{2n}{n}$ überlegen. Da er ein mittlerer Summand in

$$\sum_{k=0}^{2n} \binom{2n}{k} = 2^{2n} = 4^n, \tag{2.89}$$

und somit größer oder gleich aller $2n$ Summanden ist, muss er auch größer als der Durchschnitt $\frac{4^n}{2n}$ sein. Somit folgt nun mit allen bisherigen Überlegungen folgende Abschätzung für den Binomialkoeffizienten:

$$\frac{4^n}{2n} \leq \binom{2n}{n} \leq \prod_{p \leq \sqrt{2n}} 2n \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \cdot \prod_{n < p \leq 2n} p \tag{2.90}$$

und da es höchstens $\sqrt{2n}$ Primzahlen $p \leq \sqrt{2n}$ geben kann, schlussendlich für $n \geq 3$

$$4^n \leq (2n)^{1+\sqrt{2n}} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \cdot \prod_{n < p \leq 2n} p. \tag{2.91}$$

In einem letzten Schritt wird zunächst angenommen, das Bertrand'sche Postulat 2.3.1 wäre falsch, dass also das zweite Produkt in (2.91) gleich Eins ist. Dann setzt man (2.82) in (2.91) ein, und erhält

$$4^n \leq (2n)^{1+\sqrt{2n}} 4^{\frac{2}{3}n} \tag{2.92}$$

oder

$$4^{\frac{1}{3}n} \leq (2n)^{1+\sqrt{2n}}. \tag{2.93}$$

(2.93) ist für hinreichend großes $n$ falsch: Unter Benutzung von $a + 1 < 2^a$ gilt

$$2n = (\sqrt[6]{2n})^6 < \left( \left\lfloor \sqrt[6]{2n} \right\rfloor + 1 \right)^6 < 2^{6 \lfloor \sqrt[6]{2n} \rfloor} \leq 2^{6 \sqrt[6]{2n}}, \tag{2.94}$$

und somit erhalten wir für $n \geq 50$ (also $18 < 2\sqrt{2n}$) mit (2.91) und (2.94)

$$2^{2n} \leq (2n)^{3(1+\sqrt{2n})} < 2^{\sqrt[6]{2n}(18+18\sqrt{2n})} < 2^{20 \sqrt[6]{2n} \sqrt{2n}} = 2^{20(2n)^{2/3}}. \tag{2.95}$$

Daraus folgt $(2n)^{1/3} < 20$, also $n < 4.000$. Aus der Annahme, dass 2.3.1 falsch ist, folgt dass $n < 4.000$ sein muss. Somit gilt umgekehrt für $n \geq 4.000$ das Bertrand'sche Postulat, und nachdem es in einem ersten Schritt auch für die natürlichen Zahlen $n < 4.000$ verifiziert wurde, ist der Beweis vollständig erbracht. □

Das Lemma 2.3.3, welches im Laufe des Beweises benötigt wird, kann man sogar noch genauer fassen. Nach Rosser gilt:

**Lemma 2.3.5 (Rosser)**

$$\prod_{p\leq x} p < 2.83^x \qquad \textit{und} \qquad \prod_{p\leq x} p > 2^x \quad \textit{für } x \geq 29 \tag{2.96}$$

Zum Abschluss dieses Abschnittes werden noch drei weitere Resultate (ohne Beweis) gebracht. Zunächst kann man das Bertrand'sche Postulat mit Hilfe der Funktion $\pi(x)$, die vor allem im kommenden Kapitel genauer untersucht wird, folgendermaßen formulieren:

**Satz 2.3.6 (Tschebyschew)** *Sei $n \in \mathbb{N}^\times$ eine natürliche Zahl größer oder gleich Eins. Dann gilt*

$$\pi(2n) - \pi(n) \geq 1. \tag{2.97}$$

Wenn man noch genauer ist (siehe Satz 32 in [Tro53]), lässt sich die Differenz $\pi(2n) - \pi(n)$ etwas besser abschätzen, und man gelangt zu folgendem

**Satz 2.3.7 (von Finsler)** *Sei $n \in \mathbb{N}^\times$ eine natürliche Zahl größer als Eins. Dann gilt*

$$\frac{n}{3\ln(2n)} < \pi(2n) - \pi(n) < \frac{7n}{5\ln n}. \tag{2.98}$$

Die zweite Aussage in diesem Zusammenhang geht auf Legendre zurück, wonach folgender Satz gilt:

**Satz 2.3.8 (Legendre)** *Sei $n \in \mathbb{N}, n > 1$, dann existiert in jedem Intervall $[n, n + 2\sqrt{n}]$ mindestens eine Primzahl.*

Dieses Resultat ist freilich viel stärker als das Betrand'sche Postulat, jedoch ist letzteres weitaus berühmter.

In einem Artikel von Dusart ([Dus99]), der eigentlich erst im übernächsten Abschnitt zur Anwendung gelangt, findet sich schließlich noch folgende Aussage, mit der dieser Abschnitt schließt:

**Satz 2.3.9 (Dusart)** *Sei $n \in \mathbb{N}, n \geq 3.275$, dann liegt in jedem Intervall $\left[n, n + \frac{n}{2\ln^2 n}\right]$ zumindest eine Primzahl.*

### 2.3.2 Konstruktion von Primzahlen

Im Anschluss an das Bertrand'sche Postulat sollen zwei kurios anmutendende Sätze über Primzahlen mit gegebenen Anfangs- bzw. Endziffern vorgestellt werden.

Nach den allseits bekannten Teilbarkeitsregeln kann eine Primzahl nur mit $1, 3, 7$ oder $9$ als letzte Ziffer enden. Demgegenüber können für die erste Stelle keinerlei Einschränkungen gemacht werden, wie schon ein Blick auf die ersten 25 Primzahlen beweist.

Nun gibt es in diesem Zusammenhang sogar eine Verallgemeinerung von einer Stelle auf mehrere, denn Sierpiński hat folgenden Satz bewiesen:

**Satz 2.3.10 (Sierpiński)** *Sind $c_1, c_2, \ldots, c_m$ endlich viele Ziffern des Dezimalsystems und $c_1 \neq 0$, so gibt es beliebig viele Primzahlen, die mit der Ziffernfolge $c_1 c_2 \ldots c_m$ beginnen.*

*Beweis:* Unter Zuhilfenahme von Satz 2.1.9 lässt sich 2.3.10 sehr leicht zeigen:
Sei $a$ die aus $c_1, c_2, \ldots, c_m$ in dieser Reihenfolge gebildete $m$-ziffrige Zahl. Es genügt zu beweisen, dass

$$\lim_{n\to\infty} \{\pi[(a+1)10^n] - \pi(a \cdot 10^n)\} = \infty \tag{2.99}$$

gilt. Zu gegebenem $a$ gibt es dann beliebig viele $n$ mit

$$\pi[(a+1)10^n] - \pi(a \cdot 10^n) > 1. \tag{2.100}$$

Jede solche Ungleichung zeigt die Existenz von Primzahlen zwischen $a \cdot 10^n$ und $(a+1)10^n$, die alle mit denselben Ziffern wie $a$ beginnen. Beim Nachweis von (2.99) geht jetzt (2.19) entscheidend ein. Wegen

$$\lim_{n\to\infty} \frac{n \ln 10 + \ln(a+1)}{n \ln 10 + \ln a} = 1 \tag{2.101}$$

erhält man nach leichter Umformung

$$\lim_{n\to\infty} \frac{\pi[(a+1)10^n]}{\pi(a \cdot 10^n)} = \frac{a+1}{a} \tag{2.102}$$

oder

$$\lim_{n\to\infty} \frac{\pi[(a+1)10^n] - \pi(a \cdot 10^n)}{\pi(a \cdot 10^n)} = \frac{1}{a}. \tag{2.103}$$

Da der Nenner unendlich wird und der Quotient positiv bleibt, muss der Zähler auch unendlich werden, was zu beweisen war. □

Auch beim zweiten Satz, der ebenfalls von Sierpiński stammt, wird im ansonsten recht einfachen Beweis ein schwieriges Resultat benötigt, das erst zu einem späteren Zeitpunkt genauer vorgestellt wird (vgl. Satz 4.2.2). Deswegen ist es hier zunächst als Lemma formuliert:

**Lemma 2.3.11** *Jede arithmetische Folge $a + kd$ $(k = 0, 1, 2, \ldots)$, wo $a$ und $d$ zueinander teilerfremd sind, enthält unendlich viele Primzahlen.*

Somit folgt nun unmittelbar:

**Satz 2.3.12 (Sierpiński)** *Sind $c_1, c_2, \ldots, c_m$ endlich viele Dezimalziffern, und $c_m = 1, 3, 7$ oder $9$, so gibt es beliebig viele Primzahlen, die mit der Ziffernfolge $c_1 c_2 \ldots c_m$ enden.*

*Beweis:* Die aus $c_1 c_2 \ldots c_m$ in dieser Reihenfolge gebildete Zahl $a$ ist zu $10^m$ teilerfremd. Nach 2.3.11 gibt es also unendlich viele $p = k \cdot 10^m + a, k > 0$. Die letzten $m$ Ziffern dieser $p$ sind mit denjenigen von $a$ identisch, was zu beweisen war. □

### 2.3.3 Größe der $n$ten Primzahl $p_n$

Zum Abschluss dieses Kapitels wollen wir uns noch mit Abschätzungen für die $n$te Primzahl bechäftigen. Eines der neuesten Ergebnisse auf die Frage nach der Größe von $p_n$ wird später bei der Implementierung einer Funktion in DERIVE, die die $n$te Primzahl ausrechnen soll, behilflich sein (vgl. [Dus99]).

Ein flüchtiger Blick auf die Zahlengerade genügt, um folgendes Lemma zu „beweisen“:

**Lemma 2.3.13** *Die $n$te Primzahl $p_n$ ist stets echt größer $n$.*

Jedoch scheint diese triviale Beobachtung nicht wirklich eine befriedigende Antwort auf die Frage nach der Größe zu sein. Um die Funktion `nprime(n)` neu zu implementieren, ist man an einer besseren Abschätzung interessiert.

Wie beim Lemma 2.2.30 angemerkt, folgt aus dem Primzahlsatz 2.1.9:

$$p_n \sim n \ln n \tag{2.104}$$

Rosser (siehe [Ros39]), dem wir schon in Verbindung mit dem Bertrand'schen Postulat begegnet sind, zeigte

**Satz 2.3.14 (Rosser)** *Sei $n \geq 1$, dann gilt für die nte Primzahl $p_n$*

$$p_n \geq n \ln n. \tag{2.105}$$

Er und Schoenfeld konnten diese Aussage noch präzisieren und formulierten 1962 den

**Satz 2.3.15 (Rosser & Schoenfeld)** *Sei $n \geq 2$, dann gilt für die nte Primzahl $p_n$*

$$n(\ln n + \ln\ln n - 3/2) \leq p_n \leq n(\ln n + \ln\ln n - 1/2). \tag{2.106}$$

Im Jahre 1983 gelang Robin ([Rob83]) ein weiterer Schritt, indem er

$$p_n \geq n(\ln n + \ln\ln n - 1.0072629) \tag{2.107}$$

zeigte.

Letzterer wiederum war 1996 gemeinsam mit Massias ([MR96]) imstande, folgenden Satz zu zeigen, der schon beinahe die Aussage beinhaltet, mit der wir uns schlussendlich zufrieden geben werden.

**Satz 2.3.16 (Massias & Robin)** *Bezeichne $p_n$ wie üblich die nte Primzahl ($p_1 = 2, p_2 = 3, \ldots$), dann gilt für $2 \leq n \leq e^{598}$ und für $n \geq e^{1.800}$ die Abschätzung*

$$p_n \geq n(\ln n + \ln\ln n - 1). \tag{2.108}$$

Drei Jahre später erschien von Dusart jener Artikel [Dus99], in dem die Lücke von $e^{598}$ bis $e^{1.800}$ im obigen Satz geschlossen werden konnte, sodass die Abschätzung (2.108) nunmehr für alle $n \geq 2$ Gültigkeit besitzt.

Diese Aussage ist es auch, die im Abschnitt 3.4.6 am Ende zur Implementierung von `nprime(n)` verwendet wird.

Für weiterführende Literatur sei an dieser Stelle nochmals ausdrücklich auf den Artikel von Dusart [Dus99] und sein reichhaltiges Literaturverzeichnis hingewiesen.

Wir wollen uns jedoch nunmehr von den mehr oder weniger konkreten Betrachtungen dieses Kapitels abwenden, und uns einem anderen, nicht minder faszinierenden Gebiet der Zahlentheorie, zuwenden.

# Kapitel 3

# Der Primzahlsatz

## 3.1 Die Riemann'sche Vermutung

Wie bereits im vorangegangenen Kapitel sehr eindrucksvoll verdeutlicht wurde, besteht der überwiegende Teil der Resultate auf dem hier untersuchten Gebiet der Zahlentheorie aus zahlreichen Vermutungen, die sich zum Teil aus heuristischen Überlegungen heraus erklären lassen, die aber von einem endgültigen Beweis mehr oder weniger weit entfernt sind. Als Beispiel sei nur die Cramer'sche Vermutung erwähnt, die im Zusammenhang mit den Fortune'schen Zahlen Klarheit schaffen würde, jedoch weit außerhalb des derzeit Erreichbaren angesiedelt ist.

### 3.1.1 Definition und Eigenschaften von $\zeta(s)$

Das berühmteste Beispiel einer Vermutung, noch dazu mit „unzähligen" Auswirkungen auf die gesamte Mathematik, ist wohl die nach ihrem Schöpfer benannte Riemann'sche Vermutung, die auf den deutschen Mathematiker Bernhard Georg Friedrich Riemann (1826-1866) zurückgeht. Diese berühmte Vermutung tauchte erstmals in seiner anlässlich der Wahl zum Korrespondierenden Mitglied der Berliner Akademie der Wissenschaften eingereichten Arbeit „Über die Anzahl der Primzahlen unter einer gegebenen Größe" ([Rie59]) auf. Er betrachtete darin die Funktion

**Definition 3.1.1** *Sei $s$ eine beliebige komplexe Zahl $s = \sigma + i\tau$ mit* $\mathrm{Re}(s) = \sigma > 1$. *Dann definiert man die Funktion $\zeta(s)$ wie folgt*

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad s = \sigma + i\tau, \sigma > 1. \tag{3.1}$$

*Man nennt diese Funktion heute „Riemann'sche $\zeta$-Funktion".*

Tatsächlich konnte Riemann genau diese Funktion dazu nutzen, um Aussagen über die Primzahlverteilung zu bekommen.

Um den auf den ersten Blick nicht unmittelbar einleuchtenden Zusammenhang zwischen $\zeta(s)$ und den Primzahlen etwas zu verdeutlichen, batrachtet man folgende Identität:

**Lemma 3.1.2** *Mit den üblichen Bezeichnungen gilt für eine komplexe Zahl* $s$ *mit* $\mathrm{Re}(s) > 1$

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p^s}}, \tag{3.2}$$

Diese bereits von Euler entdeckte Beziehung war auch der Ausgangspunkt für Riemann. Die Gültigkeit von (3.2) ist sehr leicht einzusehen und folgt einem ähnlichen Gedankengang, wie der 2. Beweis des Satzes 2.1.2 von Euklid. Dazu schreibt man jeden Faktor des Produktes als (konvergente) geometrische Reihe an:

$$\frac{1}{1 - p^{-s}} = 1 + p^{-s} + p^{-2s} + p^{-3s} + \cdots . \tag{3.3}$$

Multipliziert man ein Produkt der Gestalt

$$\prod_{p \in I} \frac{1}{1 - p^{-s}} = \prod_{p \in I} \left(1 + p^{-s} + p^{-2s} + \cdots\right) \tag{3.4}$$

aus, so erhält man eine Summe über sämtliche möglichen Kombinationen von Produkten mit Faktoren aus $I$:

$$\sum (p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{|I|}^{\alpha_{|I|}})^{-s}. \tag{3.5}$$

Da in (3.2) das Produkt über alle Primzahlen gebildet wird, folgt unmittelbar

$$\prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}} = \sum_{n=1}^{\infty} n^{-s}, \tag{3.6}$$

womit (3.2) bewiesen ist.

Mit der Untersuchung von (3.1) betrat Riemann also keinesfalls Neuland. Was jedoch mit Riemann neu wurde, und worin seine Wichtigkeit begründet liegt, ist die Tatsache, dass er $\zeta(s)$ auf die gesamte Komplexe Ebene fortsetzte. Somit schuf er eine Funktion, die mit Ausnahme von $s = 1$, wo sie einen Pol erster Ordnung mit Residuum 1 besitzt, analytisch ist. Mit Hilfe des Prinzips der analytischen Fortsetzung kann man den Definitionsbereich von $\zeta(s)$ weiter ausdehnen:

$$\left.\begin{array}{rl} \zeta(s) & = 1+ \quad \frac{1}{2^s} + \frac{1}{3^s} \quad + \frac{1}{4^s} + \cdots \\ \frac{2}{2^s}\zeta(s) & = \qquad \frac{2}{2^s} \qquad + \frac{2}{4^s} + \cdots \end{array}\right\}$$

$$\Rightarrow \left(1 - 2^{1-s}\right)\zeta(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \cdots = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s}. \tag{3.7}$$

Diese Reihe konvergiert nun sogar für $\mathrm{Re}(s) > 0$, und sie stellt in dem Bereich eine analytische Funktion dar. Außer für $s = 1$ kann damit $\zeta(s)$ für alle $s$ mit $\mathrm{Re}(s) > 0$ definiert werden. Um $\zeta(s)$ schließlich auch für $\mathrm{Re}(s) \leq 0$ zu erklären, bedient man sich üblicherweise Funktionalgleichungen, wie z.B.

$$\zeta(1-s) = 2^{1-s}\pi^{-s}\cos\left(\frac{\pi s}{2}\right)\Gamma(s)\zeta(s) \tag{3.8}$$

wobei $\Gamma(s)$ die Gamma-Funktion ist (siehe Definition 1.2.3).

Riemann konnte ferner beweisen, dass $\zeta(s)$ für alle $s = -2n, n \in \mathbb{N}^{\times}$ eine einfache Nullstelle besitzt, sonst aber für alle reellen $s$ sowie für komplexe $s$ mit $\mathrm{Re}(s) = \sigma < 0$ bzw. $\sigma > 1$ von Null verschieden ist. Somit müssen also die von $s = -2n$ verschiedenen Nullstellen von $\zeta(s)$ komplexwertig sein und im Streifen $0 \leq \sigma \leq 1$ liegen.

Riemann stellte in seiner Arbeit mehrere Vermutungen auf, unter anderem, dass es im Streifen $0 \leq \sigma \leq 1$ unendlich viele Nullstellen von $\zeta(s)$ gibt, die nicht nur symmetrisch zur reellen Achse, sondern auf Grund der Funktionalgleichung (3.8) auch symmetrisch zur Geraden $\sigma = \frac{1}{2}$, verteilt liegen. Diese Vermutung wurde 1893 von Jacques Hadamard bewiesen, drei Jahre bevor dieser gleichzeitig mit De la Vallée Poussin den berühmten Primzahlsatz zeigte, dem wir uns im folgenden Abschnitt widmen wollen.

Mit der Zeit wurden die von Riemann geäußerten Vermutungen nach und nach bewiesen, mit einer Ausnahme:

**Vermutung 3.1.3 (Riemann'sche Vermutung)** *Die unendlich vielen Nullstellen der Riemann'schen Funktion $\zeta(s)$ im kritischen Streifen $0 < \mathrm{Re}(s) < 1$ liegen alle auf der Mittelgeraden $\mathrm{Re}(s) = \frac{1}{2}$.*

Sie stellt heute wohl eines der größten Rätsel in der gesamten Mathematik dar, da aus ihr zahlreiche wichtige Folgerungen in den unterschiedlichsten Gebieten gezogen werden können. So basieren beispielsweise die derzeitigen Beweisfragmente für die nicht weniger berühmte Goldbach'sche Vermutung (siehe Vermutung 2) allesamt auf ihr. Sollte sich 3.1.3 als falsch herausstellen - was jedoch allgemein bezweifelt wird - so wäre sämtlichen bisherigen Überlegungen rund um diese große Vermutung die Basis entzogen.

Es wird durchwegs davon ausgegangen, dass die Riemann'sche Vermutung richtig ist. Auch die großen Anstrengungen, die mit einer numerischen Überprüfung verbunden sind, bestätigen diese Annahme. So weiß man z.B., dass die ersten 1.500.000.001 Nullstellen exakt auf der Geraden $\mathrm{Re}(s) = \frac{1}{2}$ liegen. (Siehe dazu [Bre79],[BLRW82],[LR83],[LRW86] bzw. [21].)

### 3.1.2 Zur Berechnung der Nullstellen von $\zeta(s)$

Wie berechnet man solche Nullstellen der Riemann'schen $\zeta$-Funktion? Die effizienteste Art, die Werte von $\zeta(s)$ im kritischen Streifen (so nennt man das Gebiet $0 < \sigma < 1$) zu bestimmen, geht auf Carl Ludwig Siegel zurück, der im Jahre 1932 diese Methode vorstellte, welche er aus Riemann's unveröffentlichten Arbeiten rekonstruierte. Sie ist heute unter dem Namen „Riemann-Siegel-Formel" bekannt. Zunächst definiert man für reelles $t$:

**Definition 3.1.4** *Sei $t \in \mathbb{R}$, dann definieren wir die Funktionen $\theta(t)$ und $Z(t)$ wie folgt:*

$$\theta(t) := \arg\Gamma\left(\frac{1}{4} + \frac{it}{2}\right) - \frac{t\ln\pi}{2} \tag{3.9}$$

$$Z(t) := \zeta\left(\frac{1}{2} + it\right) e^{i\theta(t)}. \tag{3.10}$$

Wie sich herausstellt, impliziert die Funktionalgleichung

$$\zeta(1-s) = 2^s \pi^{s-1} \sin\frac{1}{2}s\pi\Gamma(1-s)\zeta(s) \tag{3.11}$$

dass $Z(t)$ reellwertig ist für $t \in \mathbb{R}$. Ferner besitzt $Z(t)$ die gleichen Nullstellen wie $\zeta(1/2 + it)$. Nach

$$\left|\zeta\left(\frac{1}{2} + it\right)\right| = |Z(t)| \tag{3.12}$$

kann man $Z(t)$ als den Graphen von $|\zeta(1/2 + it)|$ interpretieren, wobei die negativen Teile der Funktion nach unten geklappt sind, sodass eine stetige Funktion entsteht (siehe Abbildung 3.1).

Nachdem $Z(t)$ eine stetige, reelle Funktion darstellt, kann mit dem einfachen Zwischenwertsatz auf die Suche nach den Vorzeichenwechseln von $Z(t)$ gegangen werden. Vom Aufwand her benötigt die Riemann-Siegel-Formel etwa $\sqrt{t}$ Schritte um $\zeta(1/2 + it)$ zu berechnen und ist damit viel effizienter als beispielsweise die Euler-Maclaurin'sche Summenformel. Darüberhinaus können auch die Werte von größeren $t \in \mathbb{R}$ damit berechnet werden.

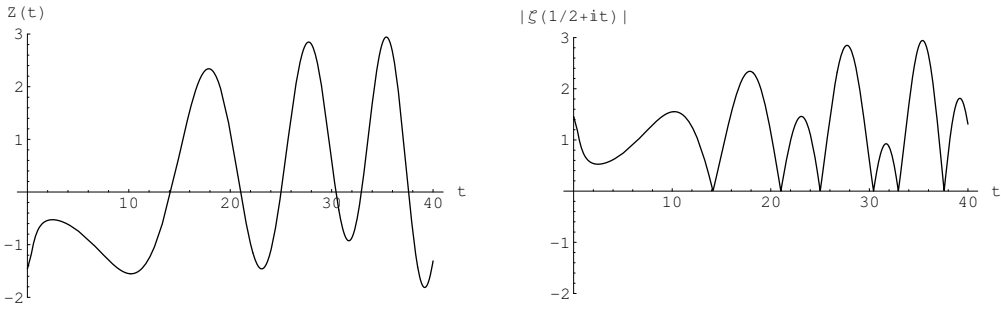


Abbildung 3.1: Die Funktionen $Z(t)$ und $|\zeta(1/2+it)|$ für $0 < t < 40$.

Später soll versucht werden, den Einfluss der komplexwertigen Nullstellen genauer zu untersuchen. Nunmehr ist klar, wie man die dazu benötigten Nullstellen erhalten kann.

Zu Beginn muss die Funktion $Z(t)$ in DERIVE implementiert werden:

```
riemannsiegelz(t) :=
  RE(ZETA(1/2+#it)EXP(#i(PHASE(GAMMA(1/4+#it/2))-tLN(pi)/2)))
```

Anschließend gilt es die Nullstellen von $Z(t)$ zu bestimmen. Da dies einen einmaligen Vorgang darstellt, erscheint es nicht sinnvoll, in die Berechnung der Nullstellen sehr viel zu investieren. So wäre beispielsweise die DERIVE-Routine `NSOLVE` bei genügender Zeit durchaus ausreichend. Je nach gewünschter Genauigkeit des Ergebnisses gelangt man etwa mittels

```
NSOLVE(riemannsiegelz(t), t, 10, 20)
```

mehr oder weniger rasch zur ersten Nullstelle von $\zeta(s)$, deren Imaginärteil mit 14.13472514173469379 zwischen den beiden Startwerten 10 und 20 liegt. Wir führen die Berechnung z.B. der ersten 50 Nullstellen einmal durch, und speichern die Imaginärteile in der Variable `zetaZeros` in Form eines Vektors ab. Für spätere Untersuchungen (siehe Abschnitt 3.3.2) wurden die Nullstellen auf etwa 70 Stellen genau berechnet (siehe Tabelle 3.1).

Dies ist vorläufig alles, was getan werden kann. Die Imaginärteile der Nullstellen sind für zukünftige Rechnungen in der Variable `zetaZeros` abgespeichert.

Weiters kennt man die Nullstellen außerhalb von $0 \leq \sigma \leq 1$. Im Zusammenhang mit der Riemann'schen Vermutung weiß man auch, dass es aus Symmetriegründen genügt, sich auf den Bereich $\frac{1}{2} \leq \sigma < 1$ zu konzentrieren.

14.13472514173469379045725198356247027078425711569924317568556721.02203963877155499262847959389690277733434052490278175462952025.01085758014568876321379099256282181865954967255799667249654230.42487612585951321031189753058409132018156002371544018096215132.93506158773918969066236896407490348881271560351703900927997137.58617815882567125721776348070533282140559735083079321833300140.91871901214749518739812691463325439572616596277727953616130343.32707328091499951949612216540680578264566837183687144687889348.00515088116715972794247274942751604168684400114442511777531249.77383247767230218191678467856372405772317829967665559208042214


Tabelle 3.1: Die Imaginärteile der ersten 10 Nullstellen der Riemann'schen $\zeta$-Funktion auf 50 Nachkommastellen berechnet.

Warum jedoch untersucht man in der Praxis „nur“ den kritischen Streifen $0 < \sigma < 1$? Was ist beispielsweise mit $\zeta(1 + it)$, und wie verhält sich die Funktion dort? Die Tatsache, wie schwierig allein der Nachweis war, dass die Zeta-Funktion auf der Gerade $\sigma = 1$ nullstellenfrei ist, zeigt abermals, wie sehr viel komplizierter sich eine fundierte Untersuchung der Riemann'schen Vermutung gestalten würde.

So einfach die Aufgabenstellung klingt, so schwierig war es, letztlich den Beweis dafür zu erbringen, dass die Riemann'sche $\zeta$-Funktion für $\mathrm{Re}(s) = 1$ keine Nullstellen besitzt, und somit auch den Beweis für einen zu dieser Aussage äquivalenten Satz in der Mathematik zu erhalten:

## 3.2 Der Primzahlsatz

Es dauerte rund ein Jahrhundert, um von den Anfängen des Satzes bis zu seinem ersten Beweis zu gelangen. Ende des 18. Jahrhunderts glaubten Legendre und der junge Gauss durch ihr Studium von zahlreichen Intervallen und den in ihnen liegenden Primzahlen eine erste Näherung $f(x)$ an die Funktion $\pi(x)$ gefunden zu haben. (Jedoch blieb es bei beiden zeit ihres Lebens bei reinen Vermutungen!) Das Wort „Näherung“ soll dabei so verstanden werden, dass das Verhältnis vom Fehler $\pi(x) - f(x)$ zum wahren Wert $\pi(x)$ für hinreichend großes $x$ beliebig klein wird. Es soll also

$$\frac{\pi(x) - f(x)}{\pi(x)} = 1 - \frac{f(x)}{\pi(x)} \tag{3.13}$$

für $x \to \infty$ einen Limes besitzen, und dieser gleich Null sein:

$$\lim_{x\to\infty} \frac{f(x)}{\pi(x)} = 1. \tag{3.14}$$

So stammt etwa von Legendre der folgende erste Ansatz:

$$\pi(x) \approx \frac{x}{\ln x - A(x)} \tag{3.15}$$

wobei Legendre der Ansicht ist, dass die Funktion $A(x)$ für $x \to \infty$ gegen den Grenzwert

$$\lim_{x\to\infty} A(x) = 1.08366\ldots \tag{3.16}$$

konvergiert. Auch Gauss ist dieser Ansatz bekannt, jedoch kann er sich trotz oder gerade wegen seiner Untersuchungen an Primzahltabellen nicht zu einer Aussage überwinden, was die Konvergenz der Funktion $A(x)$ betrifft. Statt dessen formuliert Gauss

$$\pi(x) \approx \int_2^x \frac{dt}{\ln t}, \tag{3.17}$$

beweist jedoch ebenso wie Legendre keines seiner Resultate. Heute wird der zweiten Näherung meist der folgende Ausdruck vorgezogen:

$$\mathrm{li}(x) := \int_0^x \frac{dt}{\ln t}, \tag{3.18}$$

wobei $\mathrm{li}(x)$ der *Integrallogarithmus* genannt wird. Wegen der Singularität bei $x = 1$ muss der sogenannte Cauchy'sche Hauptwert

$$\lim_{\varepsilon\to 0} \left( \int_0^{1-\varepsilon} \frac{dt}{\ln t} + \int_{1+\varepsilon}^x \frac{dt}{\ln t} \right) \tag{3.19}$$

berechnet werden, der von (3.17) nur um eine Konstante, $\mathrm{li}\,2 = 1.045\ldots$, abweicht.

Nebenbei bemerkt sind die beiden Approximationen von Legendre und Gauss sogar miteinander verbunden, denn

$$\begin{aligned} \int \frac{dt}{\ln t} &= \frac{t}{\ln t} + \int \frac{dt}{\ln^2 t} = \\ &= \frac{t}{\ln t} + \frac{t}{\ln^2 t} + 2\int \frac{dt}{\ln^3 t} = \\ &= \frac{t}{\ln t - 1} - \frac{t}{\ln^2 t(\ln t - 1)} + 2\int \frac{dt}{\ln^3 t}. \end{aligned} \tag{3.20}$$

Da die beiden letzten Terme in (3.20) von geringerer Ordnung sind als der führende Term $x/(\ln x - 1)$, gilt:

$$\lim_{x\to\infty} \frac{\operatorname{li} x}{x/\ln x} = \lim_{x\to\infty} \frac{\operatorname{li} x}{x/(\ln x - 1)} = 1. \tag{3.21}$$

Somit erscheinen beide etwa gleich gute Näherungen zu bilden.

Der erste, der einem Beweis von Satz 3.2.1 einen Schritt näher kam, war Tschebyschew um die Mitte des 19. Jahrhunderts. In einer ersten Arbeit aus dem Jahr 1851 zeigte er, dass

$$\limsup_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} \geq 1 \tag{3.22}$$

und

$$\liminf_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} \leq 1 \tag{3.23}$$

gilt. Insgesamt folgt also: Entweder

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} \tag{3.24}$$

existiert nicht, oder aber der Grenzwert ist gleich Eins. Er zog in dieser Arbeit noch eine zweite wichtige Folgerung, welche Legendre's Vermutung (3.16) über den Grenzwert von $A(x)$ widerlegte. Tschebyschew bewies nämlich: Wenn

$$\lim_{x\to\infty} A(x) \tag{3.25}$$

existiert, dann ist auch dieser Grenzwert $= 1$.

Das Hauptresultat seiner zweiten, ein Jahr später vorgelegten, Arbeit lautet: Es ist

$$\liminf_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} \geq a, \tag{3.26}$$

wobei $a$ die numerische Konstante

$$a := \ln\left(\frac{2^{\frac{1}{2}}3^{\frac{1}{3}}5^{\frac{1}{5}}}{30^{\frac{1}{30}}}\right) = 0.92129202293\ldots \tag{3.27}$$

bezeichnet. Darüberhinaus gilt auch

$$\limsup_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} \leq \frac{6}{5}a = 1.10555042752\ldots \tag{3.28}$$

Mit der heutigen Notation würde man das zweite Ergebnis von Tschebyschew wie folgt zusammenfassen:

$$\pi(x) = \Theta\left(\frac{x}{\ln x}\right). \tag{3.29}$$

Tschebyschew ist zwar einen bedeutenden Schritt näher zur Wahrheit gekommen, aber über die Existenz der Grenzwerte konnte er keinerlei Aussagen machen. Dazu musste erst noch Riemann mit seinen Ergebnissen die Denkweise der Mathematiker verändern. Wie bereits im vorhergehenden Abschnitt angedeutet, besteht sein größter Beitrag darin, dass man nach ihm mit der Theorie der Komplexen Analysis an das Problem heranging, und es schließlich auch lösen konnte.

Geschehen ist dies am Ende des 19. Jahrhunderts. Auf die Arbeiten von Riemann gestützt konnte Jacques Hadamard im Jahr 1896 folgenden

**Satz 3.2.1 (Primzahlsatz)** *Bezeichne $\pi(x)$ die Anzahl der Primzahlen, die kleiner oder gleich $x$ sind und $\mathrm{li}(x)$ den Integrallogarithmus von $x$. Dann gilt für $x \to \infty$*

$$\pi(x) \sim \mathrm{li}(x) \tag{3.30}$$

*oder anders ausgedrückt*

$$\lim_{x\to\infty} \frac{\pi(x)}{\mathrm{li}(x)} = 1. \tag{3.31}$$

beweisen. Gleichzeitig mit ihm erreichte auch De la Vallée Poussin das Ziel. Ihm alleine war es vorbehalten, folgende Fragestellung zu beantworten:

*Welche der Funktionen $\frac{x}{\ln x}$ bzw. $\mathrm{li}(x)$ ist die bessere Näherung für $\pi(x)$?*

Um die Antwort von De la Vallée Poussin zu verstehen, muss der folgende Begriff des „Näherungswerts des Integrallogarithmus in endlicher Form“ definiert werden:

$$f_q(x) := \frac{x}{\ln x} + \frac{1!x}{\ln^2 x} + \frac{2!x}{\ln^3 x} + \cdots + \frac{(q-2)!x}{\ln^{q-1} x}. \tag{3.32}$$

Er bewies nun für jedes $q$ die Relation

$$\lim_{x\to\infty} \frac{\ln^q x}{x}\left(\pi(x) - \int_2^x \frac{dt}{\ln t}\right) = 0. \tag{3.33}$$

Diese besagt also, dass $\int_2^x \frac{dt}{\ln t}$, somit auch $\mathrm{li}(x)$, die Funktion $\pi(x)$ besser darstellt, als jedes $f_q(x)$. Wir wollen aber auch (3.33) ähnlich dem Tschebyschew'schen Ergebnis noch in die heute gebräuchliche Schreibweise übersetzen, und schreiben somit

$$\pi(x) = \mathrm{li}(x) + O\left(\frac{x}{\ln^q x}\right). \tag{3.34}$$

Zum Abschluss sei noch angemerkt, dass (3.33) aus der ebenfalls von De la Vallée Poussin bewiesenen noch schärferen Formel folgt:

$$\pi(x) = \int_2^x \frac{dt}{\ln t} + O\left(xe^{-\alpha\sqrt{\ln x}}\right), \tag{3.35}$$

wobei $\alpha$ eine positive Konstante ist.

Wie aus den obigen Ausführungen ersichtlich, sind diese ersten Beweise von Satz 3.2.1 dem Gebiet der sogenannten analytischen Zahlentheorie zuzuordnen. Die Suche nach ihnen dauerte rund 100 Jahre. Nachdem diese Beweise endlich vollendet waren, benötigte man weitere 50 Jahre, bis Satz 3.2.1 auch mit „elementaren" Mitteln gezeigt werden konnte. Der Durchbruch diesbezüglich gelang A.Selberg und Paul Erdös in der Mitte des vorigen Jahrhunderts und darf als Meilenstein der elementaren Zahlentheorie bezeichnet werden (siehe dafür z.B. [Sel49], [Spe56], [Dia82]).

Auf die expliziten Beweise kann hier nicht eingangen werden. Sie sind jedoch in der einschlägigen Literatur allgegenwärtig. An dieser Stelle müssen wir uns mit einem groben geschichtlichen Abriss begnügen, und auf einige Beispiele in der Literatur verweisen, in welcher der Interssierte zusätzliche Informationen finden kann (z.B. [Lan09a],[Rie94],[Spe56],[Tro53],[New80],...).

## 3.3 Einige Approximationen von $\pi(x)$

### 3.3.1 Einfache Approximationen

Wie aus dem vorigen Abschnitt hervorgeht, ist nach dem Primzahlsatz $\pi(x)$ asymptotisch gleich $\mathrm{li}(x)$. Genauer gesagt konnte Koch vor 100 Jahren unter Annahme der Riemann'schen Vermutung folgendes beweisen

$$\pi(x) = \mathrm{li}(x) + O(\sqrt{x}\ln(x)). \tag{3.36}$$

Das bedeutet also, dass etwa die Hälfte der führenden Stellen von $\pi(x)$ mit denen von $\mathrm{li}(x)$ übereinstimmen. Für die bisher bekannten Werte von $\pi(x)$

trifft dies einigermaßen zu. Bedenkt man die Schwierigkeiten, die mit der Berechnung von $\pi(x)$ verbunden sind, ist obige Beobachtung doch recht erstaunlich.

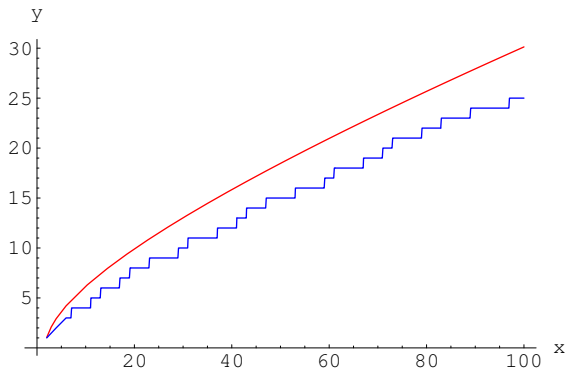


Abbildung 3.2: Die Funktionen $\mathrm{li}(x)$ und $\pi(x)$.

Wenn man einen Blick auf die Differenz $\mathrm{li}(x) - \pi(x)$ wirft, scheint diese ständig positiv zu sein. Tatsächlich war dies eine berühmte Vermutung in der Zahlentheorie, die jedoch widerlegt wurde. Littlewood bewies, dass diese Differenz ihr Vorzeichen sogar unendlich oft wechselt. Auch wenn man noch keine Zahlenwerte mit $\mathrm{li}(x) < \pi(x)$ kennt, konnte Hermann te Riele beweisen, dass zwischen $6.62 \cdot 10^{370}$ und $6.69 \cdot 10^{370}$ mehr als $10^{180}$ aufeinanderfolgende Werte $x$ liegen, mit $\mathrm{li}(x) - \pi(x) < 0$ (siehe [Rie87]).

Neueren Arbeiten von Bays und Hudson nach zu urteilen, liegen mindestens $10^{153}$ $x$-Werte in der Umgebung von $1.39822 \cdot 10^{316}$, mit $\pi(x) > \mathrm{li}(x)$ (siehe [BH99]).

Während man beim Integrallogarithmus noch keinen konkreten Wert gefunden hat, bei dem die Näherung kleiner als der tatsächliche Wert ist, so gilt für die zweite Näherung $\frac{x}{\ln x}$

$$\frac{x}{\ln x} < \pi(x) \quad \forall x \geq 11, \tag{3.37}$$

wie in der Abbildung 3.3 auf der nächsten Seite ersichtlich.

Riemann hat 1859 in seinem Artikel [Rie59] bemerkt, dass es besser ist, an Stelle von $\pi(x)$ die Funktion

$$f(x) = \sum_{n=1}^{\infty} \frac{1}{n} \pi(x^{1/n}) \tag{3.38}$$

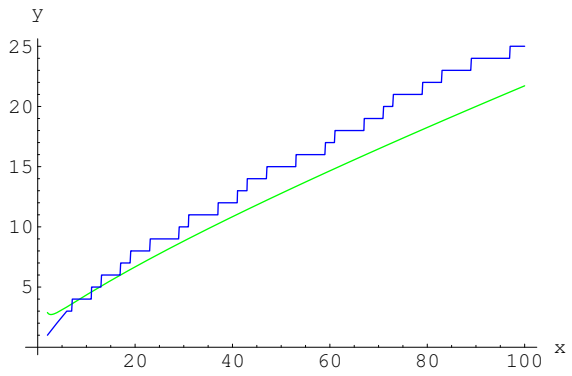


Abbildung 3.3: Die Funktionen $\frac{x}{\ln x}$ und $\pi(x)$.

zu untersuchen. Sie zählt gewissermaßen die Primzahlpotenzen $p^n$ mit $\frac{1}{n}$ gewichtet. An den Sprungstellen wird überdies der jeweilige Funktionswert derart abgeändert, dass er gleich dem arithmetischen Mittel von linksseitigem und rechtsseitigem Grenzwert ist. Bemerkenswert an $f(x)$ ist nun, dass es sich auch mit Hilfe der nichtreellen Nullstellen der Riemann'schen $\zeta$-Funktion folgendermaßen anschreiben lässt:

$$f(x) = \mathrm{li}(x) - \sum_{\zeta(\rho)=0} \mathrm{ei}(\rho \ln x) + \int_x^\infty \frac{dt}{(t^2-1)t \ln t} - \ln 2 \tag{3.39}$$

wobei $\rho$ die Nullstellen nach wachsendem Absolutbetrag geordnet durchläuft. Weiters bezeichnet $\mathrm{ei}(z)$ das Exponetialintegral, welches für ein komplexes Argument $z = u + iv, v \neq 0$ wie folgt definiert ist:

$$\mathrm{ei}(z) := \int_{-\infty+iv}^{\infty+iv} \frac{e^z}{z}\, dz. \tag{3.40}$$

Man kann aber auch die ursprüngliche Funktion $\pi(x)$ aus (3.39) zurückgewinnen:

$$\pi(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} f(x^{1/n}). \tag{3.41}$$

Dabei tritt uns hier erstmals die sogenannte Möbius'sche $\mu$-Funktion entgegen, welche für alle natürlichen Zahlen $n \neq 0$ definiert ist durch

**Definition 3.3.1 (Möbius'sche $\mu$-Funktion)** *Sei $n \neq 0$ eine natürliche Zahl. Nach dem Fundamentalsatz der Zahlentheorie 1.1.2 existiert für $n$ eine*

*Darstellung der folgenden Form*

$$n = \prod_{i=1}^{s} p_i^{\alpha_i}. \tag{3.42}$$

*Sei weiters $k$ die Anzahl der $\alpha_i$ aus (3.42), die verschieden von Null sind. Dann wird die Möbius'sche $\mu$-Funktion wie folgt definiert*

$$\mu(n) = \begin{cases} 0 & \exists i : \alpha_i \geq 2 \\ (-1)^k & \forall i : \alpha_i \leq 1 \end{cases} \tag{3.43}$$

Setzt man jetzt in (3.41) für $f(x)$ in erster Näherung wie durch (3.39) nahegelegt $\mathrm{li}(x)$ ein, so erhält man eine weitere besonders gute Approximation für $\pi(x)$:

$$R(x) := \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \mathrm{li}(x^{1/n}) \qquad (x > 0). \tag{3.44}$$

Diese Funktion wird wieder nach Riemann, der sie als Erster untersucht hat, Riemann'sche Funktion genannt. Für die Berechnung von $R(x)$ empfiehlt es sich jedoch, noch etwas weiter umzuformen, und man verwendet die durch Einsetzen von

$$\mathrm{li}(x) = \gamma + \ln\ln x + \sum_{n=1}^{\infty} \frac{(\ln x)^n}{n!n} \qquad (x > 0) \tag{3.45}$$

in (3.44) gewonnene Reihendarstellung

$$R(x) = 1 + \sum_{n=1}^{\infty} \frac{(\ln x)^n}{n!n\zeta(n+1)} \qquad (x > 0). \tag{3.46}$$

Obige Reihe konvergiert sehr rasch, sodass zur tatsächlichen Berechnung von $R(x)$ die ersten 100 Glieder in der Regel mehr als ausreichend sind. Daher ist es sinnvoll, diese ein für allemal approximativ zu bestimmen und in einem Vektor abzuspeichern. In DERIVE könnte die endgültige Implementierung von $R(x)$ unter Berücksichtigung dieser Tatsachen wie folgt aussehen:

```
r_h := APPROX(VECTOR(1 / (kZETA(k+1)k!), k, 1, 100), 20)

riemann(x) := 1 + ROUND(VECTOR(LN(x)^k_, k_, 1, 100)r_h)
```

Damit lässt sich ohne Weiteres $R(10^{10})$ berechnen. Nach 0.49 Sekunden wird das Ergebnis 455.050.683 ausgewiesen, welches vom tatsächlichen Wert von 455.052.511 nur um 1.828 oder $4 \cdot 10^{-4}\%$ abweicht. Berechnet man $R(10^9)$, so beträgt die Differenz lediglich 79 bzw. $1.5 \cdot 10^{-4}\%$!

### 3.3.2 Der Einfluss der Nullstellen von $\zeta(s)$ auf die Primzahlverteilung

Wir wenden uns nunmehr Berechnungen zu, die uns den Zusammenhang von $\zeta(s)$ und $\pi(x)$ endgültig erklären sollen. Wie schon durch (3.39) angedeutet wird, besteht eine Verbindung zwischen den Nullstellen der Riemann'schen $\zeta$-Funktion und der Anzahl der Primzahlen. Aus diesem Grund wurde auch bereits die Frage nach der Berechnung der Nullstellen von $\zeta(s)$ erörtert.

Riemann hat seinerzeit die Funktion $\pi(x)$ durch seine Funktion $R(x)$, wie sie in (3.44) definiert ist, angenähert. Tatsächlich kann nun $R(x)$ seinerseits durch Korrektur-Terme, die von der $\zeta$-Funktion abgeleitet werden, zu einer $\pi(x)$ immer besser approximierenden Funktion ausgebaut werden. Solche Berechnungen wurden erstmals von Riesel und Göhl ausgeführt (siehe [RG70]). Obwohl $R(x)$ an sich schon eine gute „grobe“ Näherung für $\pi(x)$ darstellt, konnten sie zeigen, dass die feinen Abweichungen in der Verteilung der Primzahlen durch die komplexen Nullstellen der Riemann'schen $\zeta$-Funktion gesteuert werden.

Wir halten uns im Folgenden hauptsächlich an [Wag99], in dem die Berechnungen mit Hilfe von MATHEMATICA gelöst wurden. Ein ähnlicher Gedankengang kann auch in [Rie94] nachgeschlagen werden. Bezeichne dabei $\pi_0(x)$ die von Riemann betrachtete Variante von $\pi(x)$, die sich von der ursprünglichen Funktion $\pi(x)$ eben darin unterscheidet, dass $\pi_0(p) = \pi(p) - \frac{1}{2}$ gilt für alle $p \in \mathbb{P}$. Die von Riemann vermutete und durch von Mangoldt 1895 bewiesene exakte Formel für $\pi_0(x)$ lautet:

$$\pi_0(x) = \sum_{n \geq 1} \frac{\mu(n) f(x^{1/n})}{n}. \tag{3.47}$$

Dabei ist $f(x)$ im Wesentlichen eine Summe von Integrallogarithmus und unendlich vielen Termen, die jeweils zu einer nichttrivialen Nullstelle von $\zeta(x)$ gehören. Wenn man diese Terme ignoriert, erhält man direkt die Riemann'sche Funktion $R(x)$ (siehe (3.44)).

Nun ist jedoch $\pi_0(x)$ eine Treppenfunktion, und $R(x)$ eine stetige Funktion. Riesel und Göhl hatten die Idee, für einen kleinen Bereich von $12 \leq x \leq 100$ den Einfluss eben dieser Korrekturterme, in denen die ersten 29 komplexen Nullstellen auftraten, zu untersuchen. Es zeigte sich, dass die glatte Funktion in beeindruckender Art und Weise der Treppenfunktion immer „ähnlicher“ wurde, je mehr Nullstellen, also je mehr Korrekturterme, man bei $f(x)$ in (3.47) einsetzte.

Anhand der Darstellung

$$f(x) = \mathrm{li}(x) - \sum_{\zeta(\rho)=0} \mathrm{ei}(\rho \ln x) + \int_x^\infty \frac{1}{t(t^2-1)\ln t}\,dt - \ln 2 \tag{3.48}$$

für $f(x)$, die in

$$\pi_0(x) = \sum_{n=1}^{154} \frac{\mu(n) f(x^{1/n})}{n} \tag{3.49}$$

einzusetzen ist, soll die Funktion $\pi(x)$ (resp. $\pi_0(x)$) angenähert, also die Gedankengänge von Riesel, Göhl bzw. Wagon nachvollzogen werden.

Als erschwerend wirkt sich die Tatsache aus, dass die Reihe in (3.48) nur bedingt konvergiert, ihr Wert also von der Reihenfolge der Summation abhängt. Es muss mit aufsteigendem Absolutbetrag summiert werden.

An dieser Stelle sei auch noch darauf hingewiesen, dass in (3.49) die ersten 154 Summanden einer eigentlich unendlichen Summe als Näherung betrachtet werden. Diese Wahl wird in [RG70] begründet; dort wird ebenso gezeigt, dass der entstehende Fehler mit $10^{-4}$ abgeschätzt werden kann.

Die letzten beiden Terme in (3.48) sind für große $x$ nicht sehr relevant. Riesel und Göhl zeigten, dass folgende Abschätzung gilt

$$\sum_{n=1}^{154} \frac{\mu(n)}{n} \left[ \int_{x^{1/n}}^\infty \frac{1}{t(t^2-1)\ln t}\,dt - \ln 2 \right] \approx \frac{\arctan\left(\frac{\pi}{\ln x}\right)}{\pi}. \tag{3.50}$$

Hält man sich für $f(x)$ die Formel (3.48) in (3.49) eingesetzt vor Augen, so gelangt man mit Hilfe von (3.50) schließlich zu

$$\begin{aligned}
\pi_0(x) &= \sum_{n=1}^{154} \frac{\mu(n)}{n} f(x^{1/n}) = \\
&= \underbrace{\sum_{n=1}^{154} \frac{\mu(n)}{n} \mathrm{li}(x^{1/n})}_{\approx R(x)} + \sum_{n=1}^{154} \frac{\mu(n)}{n} \left[ \int_{x^{1/n}}^\infty \frac{1}{t(t^2-1)\ln t}\,dt - \ln 2 \right] - \\
&\quad - \sum_{n=1}^{154} \frac{\mu(n)}{n} \sum_{\zeta(\rho)=0} \mathrm{ei}\left(\frac{\rho}{n} \ln x\right) \\
&\approx \underbrace{R(x) + \frac{\arctan\left(\frac{\pi}{\ln x}\right)}{\pi}}_{R^+(x):=} + \sum_{k=1}^{K} \left( - \sum_{n=1}^{154} \frac{\mu(n)}{n} \mathrm{ei}\left(\frac{\rho_k}{n} \ln x\right) \right).
\end{aligned} \tag{3.51}$$

Wir definieren also

$$R^+(x) := R(x) + \frac{\arctan\left(\frac{\pi}{\ln x}\right)}{\pi}, \tag{3.52}$$

und wenden uns der Doppelsumme in 3.51 zu, die wir zum Schluss zu $R^+(x)$ addieren. Je größer man dabei $K$ wählt, umso besser wird die Näherung sein. Die Durchnummerierung der Nullstellen erfolgt, wie schon weiter oben begründet, nach aufsteigendem Absolutbetrag geordnet, um die Konvergenz der Reihe sicherzustellen.

Man bezeichnet bei jedem Paar konjugiert komplexer Nullstellen diejenige mit positivem Imaginärteil als $\rho_1, \rho_2, \ldots$ und isoliert deren Beitrag mittels:

$$T_k(x) := -\sum_{n=1}^{154} \frac{\mu(n)}{n} \left[\mathrm{ei}\left(\frac{\rho_n}{n}\ln x\right) + \mathrm{ei}\left(\frac{\overline{\rho_n}}{n}\ln x\right)\right]. \tag{3.53}$$

Um die Berechnung von $T_k(x)$ zu beschleunigen, wird folgende Eigenschaft benutzt:

$$\mathrm{ei}(c\rho) + \mathrm{ei}(c\bar{\rho}) = \mathrm{ei}(c\rho) + \overline{\mathrm{ei}(c\rho)} = 2\,\mathrm{Re}(\mathrm{ei}(c\rho)), \tag{3.54}$$

die schließlich zu

$$T_k(x) = -2\sum_{n=1}^{154} \frac{\mu(n)}{n}\,\mathrm{Re}\left[\mathrm{ei}\left(\frac{\rho_n}{n}\ln x\right)\right] \tag{3.55}$$

führt. $T_k(x)$ steht also für den Beitrag der beiden Nullstellen $\frac{1}{2} \pm i\alpha_k$, wobei $\alpha_k$ den $k$ten Imaginärteil bezeichnet.

Durch die vorstehenden Ausführungen es ist nunmehr möglich, die Implementierung in DERIVE vorzunehmen.

In einem ersten Schritt wurden die Nullstellen der Riemann'schen $\zeta$-Funktion berechnet (siehe Tabelle 3.1). Somit kann sofort die Implementierung von (3.52) begonnen werden. Die Riemann'sche Funktion $R(x)$ ist bereits als `riemann(x)` programmiert und wird an dieser Stelle verwendet.

```
rplus(x) := riemann(x) + ATAN(PI/LN(x))/PI
```

Nach diesem sehr einfachen Ergebnis müssen wir uns jetzt mit der Funktion des Exponentialintegrals auseinandersetzen. Die standardmäßige Implementierung in DERIVE sieht wie folgt aus:

```
EI(x, m) := LN(x) + EULER_GAMMA + SUM(x^n_/(n_n_!), n_, 1, m)
```

Man bedient sich dabei also der Darstellung

$$\mathrm{ei}(x) = \ln(x) + \gamma + \sum_{n=1}^{\infty} \frac{x^n}{n \cdot n!}. \tag{3.56}$$

Will man eine vernünftige Näherung für das Exponentialintegral gewährleisten, ist es notwenig, mit sehr hoher Genauigkeit zu rechnen. Aus diesem Grund wurde auch ein Steuerungsparameter $m$ mitimplementiert, der sozusagen eine manuelle Mitbestimmung, wieweit die Reihe ausgewertet wird, ermöglicht.

Es ist jedoch unmöglich, bei einer derartigen Fülle von Rechnungen und Aufrufen von `EI(x,m)`, *einen* geeigneten Wert für `m` zu finden. Wählt man ihn zu klein, stimmen die Werte für größeres $x$ nicht; wählt man ihn zu groß, werden für kleine $x$-Werte viel zu viele Rechenschritte unnötigerweise ausgeführt, sodass das Ergebnis zu lange auf sich warten lässt.

Es erscheint somit sinnvoll, die Funktion `EI(x,m)`, welche etwas rudimentär implementiert ist, in „intelligenter“ Art und Weise auszubauen. Das Ziel ist es, eine Funktion zu schreiben, die sich der gleichen Näherung (3.56) bedient, wie das Original, die jedoch sobald die gewünschten Stellen stehen, automatisch abbricht. Dadurch wird erreicht, dass für kleine und große $x$ nur die notwendige Anzahl an Reihengliedern berechnet werden.

Weiters genügt es, den Realteil des Exponentialintegrals zu kennen, sodass man sich bei dessen Berechnung auf die Realteile konzentrieren kann. Die Umsetzung all dieser Gedanken in DERIVE könnte schließlich so aussehen:

```
eire(x, a_ := 0, b_ := 0, n_ := 1) :=
  Prog
    b_ := EULER_GAMMA + RE(LN(x))
    Loop
      b_ :+ RE(x^n_)/(n_n_!)
      If APPROX(a_ = b_)
         RETURN a_
      a_ := b_
      n_ :+ 1
```

Mit dieser Realisierung konnte jedoch die hohe Sensibilität des Ergebnisses in Bezug auf die Rechengenauigkeit nicht vermieden werden. Wenn wir z.B. in einer Genauigkeit von 50 Stellen rechnen, was durch folgende Zeile erreicht wird

```
PrecisionDigits := 50
```

so ergibt sich für $\mathrm{ei}\left(\frac{\rho_5}{1}\ln(100)\right)$ das offensichtlich falsche Ergebnis

```
eire((0.5 + #izetaZeros SUB 5)/1LN(100))=
-7.092282778793526161188377836553051358954918586944 8·10^11.
```

Tatsächlich ist es hier notwendig, die Berechnungen auf mehr Stellen genau auszuführen. Setzt man etwa

```
PrecisionDigits := 75,
```

so kommt bereits ein vernünftigeres Resultat zum Vorschein:

$$\mathrm{ei}\left(\frac{\rho_5}{1}\ln(100)\right) = 0.050967467998460551318060507156558366 61\ldots \quad (3.57)$$

Weiters kann an diesem Beispiel die große Stärke von `eire(x)` gegenüber `EI(x,m)` gezeigt werden.

Im Zuge der Berechnung von $T_5(x)$ für $12 \leq x \leq 100$, wie sie später durchgeführt werden, ist es notwendig, sowohl

$$\mathrm{ei}\left(\frac{\rho_5}{1}\ln(100)\right) \approx 0.0509674704 \quad (3.58)$$

als auch

$$\mathrm{ei}\left(\frac{\rho_5}{154}\ln(12)\right) \approx -0.1169195958 \quad (3.59)$$

zu bestimmen.

Unter Verwendung der alten, eingebauten Variante `EI(x,m)` muss `m` ein für allemal fest gewählt werden. Es stellt sich jedoch heraus, dass für $\mathrm{ei}\left(\frac{\rho_5}{1}\ln(100)\right)$ 549 Glieder in der Reihe (3.56) auszuwerten sind. Man müsste also sämtliche Berechnungen etwa mit `m=550` durchführen, wenn man die eingebaute Variante des Exponentialintegrals verwenden wollte. Hingegen genügen bei $\mathrm{ei}\left(\frac{\rho_5}{154}\ln(12)\right)$ schon die ersten 38 Reihenglieder, sodass ein Funktionsaufruf von `EI(x,550)` weit überzogen erscheint.

Aber selbst bei dem direkten Vergleich von `eire(x)` und `RE(EI(x,m))` für gleiche Werte von $x$ und $m$ schneidet die neue Variante besser ab. Auch wenn am Rechenvorgang nichts grundlegend geändert wurde, so genügen diese Verbesserungen schon, um auch in DERIVE das Exponentialintegral mit vernünftigem Aufwand auszuwerten.

Bevor wir uns der abschließenden Berechnung der $T_k(x)$ zuwenden, wollen wir uns noch eine weitere Möglichkeit überlegen, die Rechenzeit zu optimieren. Bei Betrachtung der zu berechnende Größe

$$T_k(x) = -2\sum_{n=1}^{m} \frac{\mu(n)}{n} \operatorname{Re}\left[\operatorname{ei}\left(\frac{\rho_n}{n}\ln x\right)\right], \tag{3.60}$$

erkennt man, dass die unter Umständen nach wie vor aufwendige Berechnung von $\operatorname{Re}\left[\operatorname{ei}\left(\frac{\rho_n}{n}\ln x\right)\right]$ im Falle von $\mu(n) = 0$ überflüssig ist. Es scheint somit sinnvoll, für fixes $m$ (in dieser Arbeit wird $m = 154$ gesetzt) jene $n$ zu bestimmen, für die $\mu(n) \neq 0$ gilt. Nur für solche $n$ ist es notwendig, das Exponentialintegral auszuwerten.

Die Moebiu'sche $\mu$-Funktion von $n$ ist dann und nur dann gleich Null, wenn die Zahl $n$ durch ein Quadrat teilbar ist. Die Wahrscheinlichkeit, dass $n$ nicht durch ein Quadrat $d^2$ teilbar ist, beträgt bekanntermaßen

$$1 - \frac{1}{d^2}. \tag{3.61}$$

Unter der Annahme, dass die Teilbarkeit durch verschiedene Zahlen voneinander unabhängige Ereignisse sind, ergibt sich somit für die Wahrscheinlichkeit, dass $n$ quadratfrei ist, folgender Ausdruck

$$\prod_{p\in\mathbb{P}} \left(1 - \frac{1}{p^2}\right). \tag{3.62}$$

Wir wissen jedoch aus (3.2), dass folgende Beziehung gilt:

$$\prod_{p\in\mathbb{P}} \left(1 - \frac{1}{p^2}\right) = \frac{1}{\sum\limits_{k=1}^{\infty} \frac{1}{k^2}} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2} \approx 0.6079271, \tag{3.63}$$

sodass wir in etwa mit $0.608 \cdot m$ Zahlen $n$ rechnen können, die übrig bleiben. Tatsächlich bleiben für $m = 154$ genau 94 $n$ übrig, bei denen $\mu(n) \neq 0$ gilt, im Vergleich zu $0.608 \cdot 154 = 93.682$. Dies liegt sehr nahe dem erwarteten Wert, und man erreicht eine Einsparung von fast 40% gegenüber einer herkömmlichen Implementierung.

Bei der Berechnung der verbleibenden $\mu(n)$ werden zusätzlich zu den $n$ die Größen $-2\frac{\mu(n)}{n}$ in zwei globalen Variablen abgelegt, sodass sie für fixes $m$ nur einmal berechnet werden müssen.

Dazu definiert man diese in DERIVE zunächst:

```
[mupos :=, muval :=]
```

Wie aus den Namen hervorgeht, werden in `mupos` die Positionen, also jene $n$, abgespeichert, für die später noch das Exponentialintegral zu bestimmen ist, und in `muval` die zugehörigen Werte $-2\frac{\mu(n)}{n}$.

```
setmu(m, n_ := 1) :=
  Prog
    mupos := []
    muval := []
    Loop
      If MOEBIUS_MU(n_) /= 0
         Prog
           mupos := ADJOIN(n_, mupos)
           muval := ADJOIN(- 2 MOEBIUS_MU(n_)/n_, muval)
      If n_ = m exit
      n_ :+ 1
```

Um die Vorbereitungen für die Berechnungen mit $m = 154$ zu treffen, genügt also jetzt der einfache Aufruf `setmu(154)`. Danach sind die Variablen `mupos` und `muval` ein für allemal gesetzt, und können für die weiteren Berechnungen, also für alle Nullstellen, verwendet werden. Erst bei einer neuen, anderen Wahl für $m$ muss die Funktion entsprechend neu aufgerufen werden.

Nunmehr kann das Augenmerk auf die Implementierung von $T_k(x)$ gerichtet werden. Voraussetzung ist neben der Initialisierung von `mupos` und `muval` auch die von `zetaZeros`, in der die Imaginärteile der Nullstellen von $\zeta(s)$ abgelegt sind. Dann ergibt sich die Berechnung von $T_k(x)$ in zwei Schritten.

Zunächst bestimmt man die Werte $\mathrm{Re}\left[\mathrm{ei}\left(\frac{\rho_n}{n}\ln x\right)\right]$ wie folgt:

```
Tmu(x, k, r_, l_ := [], p_) :=
  Prog
    p_ := mupos
    r_ := 0.5 + #i zetaZerosSUBk
    Loop
      l_ := ADJOIN(eire(r_/FIRST(p_)LN(x)), l_)
      p_ := REST(p_)
      If p_ = []
         RETURN REVERSE l_
```

In einem letzten Schritt werden die Zwischenresultate zu einem Endergebnis vereinigt:

```
T(x, k) := FIRST(FIRST([Tmu(x, k)][muval]‘))
```

Somit ist die Berechnung der Größen $T_k(x)$ in DERIVE endgültig implementiert.

Bevor wir uns die Auswirkung auf $\pi(x)$ anschauen, wollen wir einige Graphen von $T_k(x)$ in Abbildung 3.4 aufzeichnen.

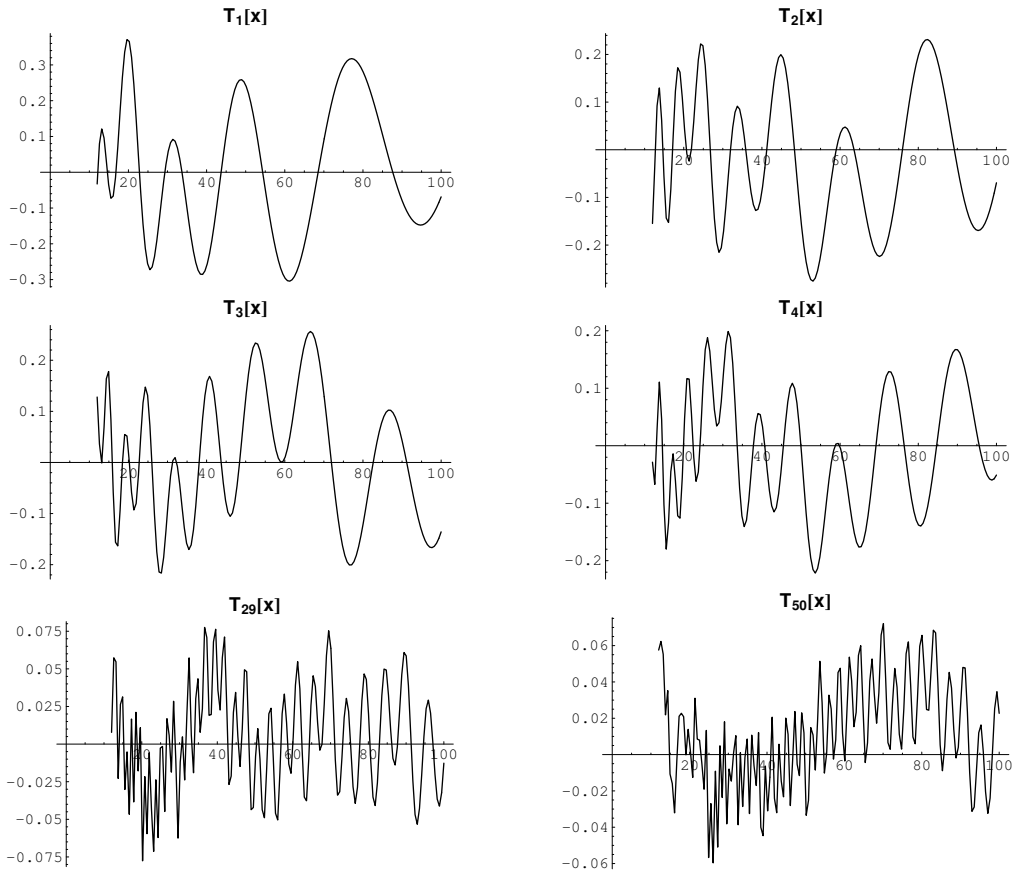


Abbildung 3.4: Die Korrekturterme $T_k(x)$ zu den verschiedenen Nullstellen der Riemann'schen $\zeta$-Funktion, für $12 \leq x \leq 100$ und $k \in \{1, 2, 3, 4, 29, 50\}$.

Schließlich ergibt sich mit Hilfe von (3.51) und (3.52)

$$\pi_0(x) = R^+(x) + \sum_{k=1}^{K} T_k(x), \tag{3.64}$$

sodass zum Schluss sehr einfach die Korrekturterme der Nullstellen in die Berechnung von $\pi_0(x)$ einfließen. Die abschließende DERIVE-Routine könnte so aussehen:

```
pi_null(x, k) := rplus(x) + SUM(T(x,k_), k_, 1, k)
```

Es wird dabei mit dem Parameter `k` die Anzahl der berücksichtigten Nullstellen von $\zeta(s)$ gesteuert.

Mit Hilfe dieser Programme kann man sich mühelos die Korrekturterme zeichnen lassen (siehe Abbildung 3.4). Weiters kann auch $\pi_0(x,k)$ für verschiedene $k$-Werte einfach aufgezeichnet werden:

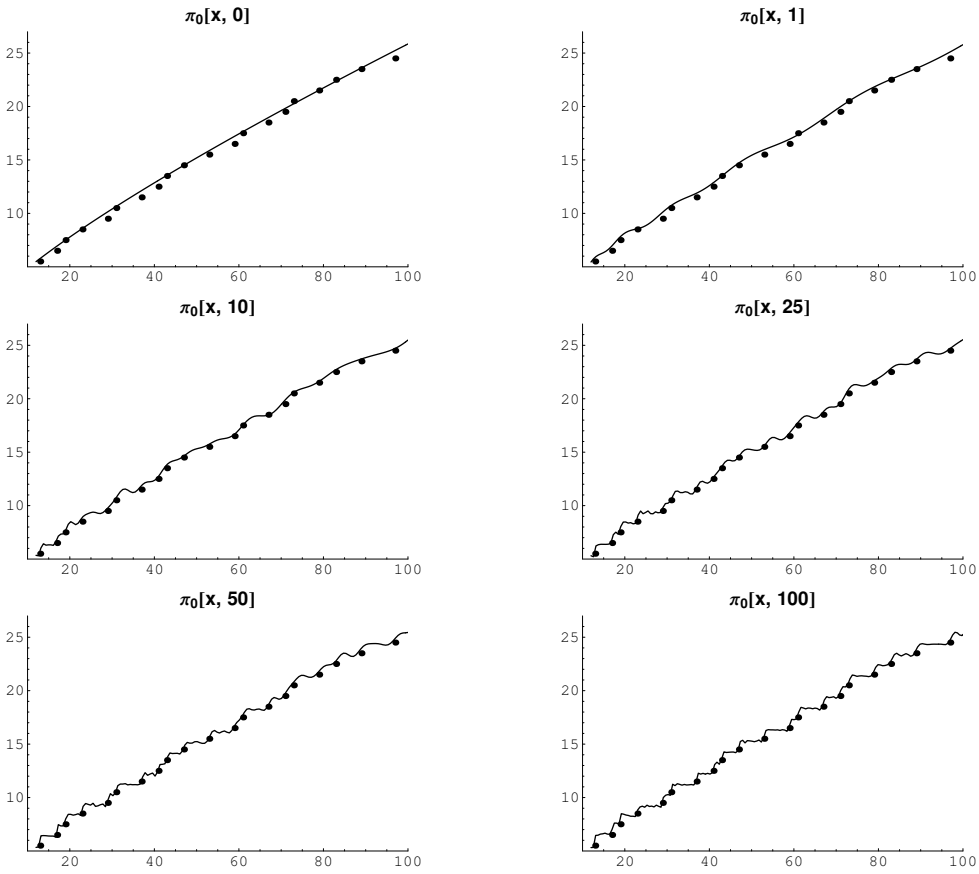


Abbildung 3.5: Die Funktionen $\pi_0(x,k)$ nach (3.49), wobei für $f(x)$ in (3.48) die ersten $k$ Korrekturterme $T_k(x)$ zu den ersten k komplexen Nullstellen $\rho_k$ verwendet wurden ($k \in \{0,1,10,25,50,100\}$).

Je mehr Nullstellen man in die Berechnungen einfließen lässt, umso genauer schmiegt sich die stetige Funktion der Treppenfunktion an (siehe Abbildung 3.5). Wie man beim Betrachten der Abbildungen sofort sieht, nimmt der

Einfluss der einzelnen Nullstellen immer mehr ab. Weiters beginnen die Nullstellen zunächst für kleine $x$ zu „greifen“, und erst später tritt auch für größere $x$-Werte eine Änderung ein. Mit den 100 zuletzt betrachteten Nullstellen lässt sich $R(x)$ auch für $x > 100$ bemerkenswert gut an $\pi_0(x)$ approximieren.

Somit wurde der Zusammenhang der komplexen Nullstellen der Riemann'schen $\zeta$-Funktion und der Funktion $\pi(x)$ (bzw. $\pi_0(x)$) ausführlich dargelegt.

## 3.4 Berechnung von $\pi(x)$

Im Gegensatz zu den eben betrachteten Approximationen für $\pi(x)$ stehen im Folgenden Möglichkeiten im Mittelpunkt, den genauen Wert von $\pi(x)$ zu eruieren. Tatsächlich gibt es mehrere Algorithmen, mit denen man die Anzahl der Primzahlen kleiner oder gleich einer gewissen Größe $x$ berechnen kann. Diese Tatsache wurde bereits im vorigen Kapitel erwähnt.

Trotz gewaltiger Fortschritte ist es nach wie vor eine sehr aufwendige Berechnung, sodass man die Werte von $\pi(x)$ erst für relativ wenige und kleine $x$ kennt. Bevor einige der Methoden zur Berechnung von $\pi(x)$ genauer betrachten werden, sind mit der Tabelle 3.2 derzeit bekannten Werte vorangestellt.

| $x$ | $\pi(x)$ | $x$ | $\pi(x)$ |
|---|---|---|---|
| $10^1$ | 4 | $10^{12}$ | 37.607.912.018 |
| $10^2$ | 25 | $10^{13}$ | 346.065.536.839 |
| $10^3$ | 168 | $10^{14}$ | 3.204.941.750.802 |
| $10^4$ | 1.229 | $10^{15}$ | 29.844.570.422.669 |
| $10^5$ | 9.592 | $10^{16}$ | 279.238.341.033.925 |
| $10^6$ | 78.498 | $10^{17}$ | 2.623.557.157.654.233 |
| $10^7$ | 664.579 | $10^{18}$ | 24.739.954.287.740.860 |
| $10^8$ | 5.761.455 | $10^{19}$ | 234.057.667.276.344.607 |
| $10^9$ | 50.847.534 | $10^{20}$ | 2.220.819.602.560.918.840 |
| $10^{10}$ | 455.052.511 | $10^{21}$ | 21.127.269.486.018.731.928 |
| $10^{11}$ | 4.118.054.813 | $10^{22}$ | 201.467.286.689.315.906.290 |

Tabelle 3.2: $\pi(x)$ für $x = 10^n, n = 1, \ldots, 22$.

### 3.4.1 Formel von Legendre

Wie wir noch sehen werden, ist das Auswerten dieser überaus wichtigen zahlentheoretischen Funktion äußerst kompliziert und vor allem arbeitsintensiv. Früher wurde $\pi(x)$ nicht selten durch einfaches Abzählen der Primzahlen $\leq x$ „berechnet". Aber durch oftmalige Fehler in den damaligen Primzahltabellen kam man nicht selten zu falschen Ergebnissen.

Zu Beginn steht die einfachste, jedoch leider gleichzeitig auch aufwendigste Methode der Berechnung. Sie wurde seinerzeit von Legendre entdeckt, und basiert auf folgender Gleichung:

$$1+\pi(x)= \pi(\sqrt{x})+\lfloor x\rfloor-\sum_{p_i\leq\sqrt{x}}\left\lfloor\frac{x}{p_i}\right\rfloor+\sum_{p_i<p_j\leq\sqrt{x}}\left\lfloor\frac{x}{p_ip_j}\right\rfloor-\sum_{p_i<p_j<p_k\leq\sqrt{x}}\left\lfloor\frac{x}{p_ip_jp_k}\right\rfloor+\cdots \quad (3.65)$$

Die Formel von Legendre ist beinahe selbsterklärend. Der Grundgedanke dahinter ist folgender:

Eins + die Anzahl der Primzahlen = die Anzahl aller ganzen Zahlen - die Anzahl aller zusammengesetzter Zahlen im Intervall $[1, x]$.

Nachdem sämtliche zusammengesetzten Zahlen in diesem Intervall einen Primfaktor $\leq \sqrt{x}$ besitzen, ist $\sum_{p_i\leq\sqrt{x}}\left\lfloor\frac{x}{p_i}\right\rfloor$ genau die Anzahl jener Zahlen des Intervalls, die Vielfache von Primzahlen sind. Darin enthalten sind jedoch auch die Primzahlen selbst, sodass $\pi(\sqrt{x})$ wieder hinzugezählt werden muss.

Weiters besteht die Möglichkeit, dass eine Zahl durch 2 Primzahlen $p_i, p_j$ teilbar ist. Diese Zahl wird derzeit zweimal abgezogen, da sie sowohl als Vielfaches von $p_i$ als auch von $p_j$ in der ersten Summe zweimal gezählt wird. Somit muss sie einmal wieder hinzugezählt werden. Diese Tatsache erklärt den Summanden $\sum_{p_i<p_j\leq\sqrt{x}}\left\lfloor\frac{x}{p_ip_j}\right\rfloor$. Durch diesen Term werden jetzt jedoch all jene zusammengesetzten Zahlen, die durch drei Primzahlen $p_i, p_j, p_k \leq \sqrt{x}$ geteilt werden, nicht weiter berücksichtigt, sodass sie wieder einmal abgezogen werden müssen, usw.

Bevor etwaige Schwierigkeiten bei der Berechnung nach Legendre aufgezeigt werden, und diese Idee in DERIVE implementiert wird, soll zunächst in einem einfachen Beispiel $\pi(100)$ bestimmt werden:

$$\begin{aligned}
\pi(100) &= \pi(10) + 100 - \left\lfloor\frac{100}{2}\right\rfloor - \left\lfloor\frac{100}{3}\right\rfloor - \left\lfloor\frac{100}{5}\right\rfloor - \left\lfloor\frac{100}{7}\right\rfloor \\
&\quad + \left\lfloor\frac{100}{2\cdot 3}\right\rfloor + \left\lfloor\frac{100}{2\cdot 5}\right\rfloor + \left\lfloor\frac{100}{2\cdot 7}\right\rfloor + \left\lfloor\frac{100}{3\cdot 5}\right\rfloor + \left\lfloor\frac{100}{3\cdot 7}\right\rfloor + \left\lfloor\frac{100}{5\cdot 7}\right\rfloor \\
&\quad - \left\lfloor\frac{100}{2\cdot 3\cdot 5}\right\rfloor - \left\lfloor\frac{100}{2\cdot 3\cdot 7}\right\rfloor - \left\lfloor\frac{100}{2\cdot 5\cdot 7}\right\rfloor - \left\lfloor\frac{100}{3\cdot 5\cdot 7}\right\rfloor \\
&\quad + \left\lfloor\frac{100}{2\cdot 3\cdot 5\cdot 7}\right\rfloor - 1 \\
&= 4 + 100 - 50 - 33 - 20 - 14 + 16 + 10 + 7 + 6 + 4 + 2 \\
&\quad -3 - 2 - 1 - 0 + 0 - 1 \\
&= 25. \qquad (3.66)
\end{aligned}$$

Wie man sich leicht vorstellen kann, stellt die Vielzahl an vorkommenden Termen bei der Berechnung nach (3.65) eine große Hürde dar, sodass diese Variante für eine oftmalige Anwendung unbrauchbar scheint.

Tatsächlich geht die erste Weiterentwicklung dieser Formel noch auf Legendre selbst zurück, der schließlich imstande war, $\pi(10^6)$ auszurechnen. Sein Wert lag mit 78.525 etwas neben der tatächlichen Anzahl von 78.498 - ein weiterer Hinweis auf die Schwierigkeiten, mit denen man bei dieser Form der Berechnung zu kämpfen hat.

Um den direkten Weg in DERIVE zu implementieren, benötigen wir zunächst eine Hilfsroutine `prod(a)`, die uns sämtliche Kombinationen an Produkten mit Faktoren aus dem Eingabevektor zurückliefert:

```
prod(a) :=
  If DIM(a) = 1
     APPEND(a)
     APPEND([FIRST(a)]‘[prod(REST(a))])
```

Damit ist es nunmehr möglich, die Funktion `leg(x,k)` zu schreiben. Sie berechnet die Primzahlen kleiner oder gleich $x$ nach (3.65), wobei der Parameter $k$ die maximale Anzahl an verschiedenen Primzahlen bezeichnet, die bei der Summation berücksichtigt werden:

```
leg(x, k, a_ := [], i_ := 0, p_, q_, s_) :=
  Prog
    s_ := PRIMEPI(SQRT(x)) + FLOOR(x) - 1
```

```
p_ := SELECT(PRIME(q), q, 1, SQRT(x))
Loop
  a_ := INSERT(p_, a_)
  i_ :+ 1
  q_ := SELECT(SQUAREFREE(q), q, prod(a_))
  q_ := VECTOR(i, i, MAP_LIST(qSUBj, j, {1, ..., DIM(q_)}))
  s_ :+ (-1)^i_SUM(FLOOR(x/q), q, q_)
  If i_ = k
     RETURN s_
```

Da später der Algorithmus nach Legendre ein zweites Mal, auf eine effizientere Art und Weise, implementiert wird, soll an dieser Stelle nicht all zu ausführlich auf die oben angeführten Programme eingegangen werden. So ist auch zu erklären, warum in `leg(x,k)` die Funktion `PRIMEPI` verwendet wurde, die DERIVE-intern die Anzahl der Primzahlen berechnet.

Wollte man ein genaues Resultat - ohne Rücksicht auf den Aufwand, der dabei betrieben wird - so müsste man offensichtlich $k = \pi(\sqrt{x})$ wählen. Aus der vorangegangenen händischen Berechnung von $\pi(100)$ (siehe (3.66)) geht jedoch hervor, dass jener Term mit allen 4 Primzahlen 2, 3, 5 und 7 nichts zur Summe beiträgt. Infolgedessen ist es vollkommen ausreichend, `leg(100,k)` mit `k`=3 aufzurufen, ohne ein falsches Resultat zu riskieren:

`leg(100,3) = 25` (0.03 Sekunden)

Der gleiche Aufruf mit $x = 1.000$ liefert folgendes Ergebnis

`leg(1000,3) = 145` (0.781 Sekunden)

Da $\left\lfloor \frac{1.000}{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11} \right\rfloor = 0$ gilt, und somit sämtliche Terme, bei denen mehr als 4 Primzahlen mitspielen, verschwinden, genügt es hier einen Aufruf mit $k = 4$ zu starten, um das richtige Ergebnis von $\pi(1.000)$ zu erhalten:

`leg(1000,4) = 168` (13.9 Sekunden)

Der Zeitaufwand steigt jedoch sprunghaft an, sodass wir uns im Folgenden mit etwas effizienteren Methoden beschäftigen wollen.

### 3.4.2 Meissel's Variante

Der erste, der einen wichtigen Schritt weiter kam, und durch eine geschickte Modifikation von Legendre's Weg $\pi(x)$ für die Werte $10^7, 10^8$ und $10^9$ berechnen konnte, war Meissel ([Mei70], [Mei71],[Mei83] und [Mei85]). Allerdings

waren auch seine Arbeiten nicht fehlerfrei, und der wohl am öftesten in der Literatur auftauchende falsche Wert geht auf ihn zurück. Im Jahre 1885 veröffentlichte er sein Ergebnis: $\pi(10^9) = 50.847.478$. Der Fehler blieb lange Zeit unbemerkt. Erst im Jahre 1958 korrigierte ihn D.E.Lehmer auf $\pi(10^9) = 50.847.534$.

Die Berechnungsweise nach Meissel stützt sich auf eine Analyse der Größen $P_k(x, a)$. Darunter versteht man die Anzahl natürlicher Zahlen zwischen 1 und $x$, die als Produkt von genau $k$ (nicht notwendigerweise verschiedener) Primfaktoren $> p_a$, also der $a$-ten Primzahl, darstellbar sind. Durchläuft $k$ die Zahlen $1, 2, 3, \ldots$, dann zählen diese Ausdrücke genau jene Zahlen im Intervall $[1, x]$, die keinen Primfaktor $q \leq p_a$ besitzen. Die $\lfloor x \rfloor$ natürlichen Zahlen im Intervall $[1, x]$ setzen sich somit wie folgt zusammen:

1. Die Eins.
2. Die ersten $a$ Primzahlen $p_1 = 2, p_2 = 3, p_3 = 5, \ldots, p_a$.
3. $\sum\limits_{1 \leq i \leq a} \left\lfloor \frac{x}{p_i} \right\rfloor - \sum\limits_{1 \leq i < j \leq a} \left\lfloor \frac{x}{p_i p_j} \right\rfloor + \cdots - a$ zusammengesetzte Zahlen, die zumindest einen Primfaktor $\leq p_a$ besitzen.
4. $P_1(x, a) = \pi(x) - a$ Primzahlen p, mit $p_a < p \leq x$.
5. $P_2(x, a)$ Zahlen $n = p_i p_j \leq x$ mit $a + 1 \leq i \leq j$.
6. $P_3(x, a)$ Zahlen $n = p_i p_j p_k \leq x$ mit $a + 1 \leq i \leq j \leq k$.

$$\vdots$$

Zählt man all das zusammen, gelangt man zu folgendem Ergebnis:

$$1 + \sum_{1 \leq i \leq a} \left\lfloor \frac{x}{p_i} \right\rfloor - \sum_{1 \leq i < j \leq a} \left\lfloor \frac{x}{p_i p_j} \right\rfloor + \sum_{1 \leq i < j < k \leq a} \left\lfloor \frac{x}{p_i p_j p_k} \right\rfloor - \cdots + \\ + \pi(x) - a + P_2(x, a) + P_3(x, a) + \cdots = \lfloor x \rfloor. \tag{3.67}$$

Zunächst wollen wir uns überlegen, wieviele der neuen Terme $P_k(x, a)$ zu berücksichtigen sind. Es ist offensichtlich, dass dies von der Wahl des Parameters $a$ abhängt. Wählt man $a$ so groß, dass $p_{a+1} > \sqrt{x}$ gilt, dann verschwindet bereits $P_2(x, a)$. Nach Definition ist $P_2(x, a)$ die Anzahl der Zahlen $\leq x$, die als Produkt von genau zwei Primzahlen $p_i, p_j \geq p_{a+1}$ dargestellt werden können. Nun gilt jedoch $p_i p_j > \sqrt{x}\sqrt{x} = x \ \forall i, j \geq a + 1$, wodurch $P_2(x, a) = 0$ folgt. Wählt man $a$ derart, dann entsteht die ursprüngliche Formel von Legendre.

Wählt man $a$ derart, dass $x^{\frac{1}{3}} < p_{a+1} < x^{\frac{1}{2}}$, so ist $P_2(x,a) \neq 0$, jedoch enthält nach einem ähnlichen Argument wie vorher $P_3(x,a)$ keine Elemente mehr, da $p_i p_j p_k > x^{\frac{1}{3}} x^{\frac{1}{3}} x^{\frac{1}{3}} > x$ gilt.

Allgemein gilt $P_r(x,a) = 0$ und $P_{r-1}(x,a) \neq 0$, falls $a$ folgendermaßen gewählt ist: $x^{\frac{1}{r}} < p_{a+1} < x^{\frac{1}{r-1}}$. Somit scheint es vernünftig zu sein, $a = \pi(x^{\frac{1}{r}})$ für ein passendes $r$ zu wählen. Man erreicht dadurch, dass $p_{a+1}$ gerade größer ist als $x^{\frac{1}{r}}$, und deswegen $P_r(x,a)$ verschwindet, die Formel (3.67) insgesamt also abbricht.

Um zur Formel von Meissel zu gelangen, wollen wir uns im Folgenden mit $P_2(x,a)$ genauer auseinandersetzen. $P_2(x,a)$ ist definiert als Anzahl der Zahlen im Intervall $[1,x]$, die das Produkt von zwei Primzahlen $p_i$ und $p_j$ mit $a+1 \leq i \leq j$ sind. Wählt man die erste Primzahl fest, so ergibt sich

$$\begin{aligned} P_2(x,a) &= \text{Anzahl der Zahlen } p_{a+1}p_j \leq x \text{ mit } a+1 \leq j \\ &\quad + \text{Anzahl der Zahlen } p_{a+2}p_j \leq x \text{ mit } a+2 \leq j \\ &\quad + \cdots \\ &= \pi\left(\frac{x}{p_{a+1}}\right) - a + \pi\left(\frac{x}{p_{a+2}}\right) - (a+1) + \cdots \\ &= \sum \left(\pi\left(\frac{x}{p_i}\right) - (i-1)\right), \end{aligned} \tag{3.68}$$

wobei für $i$ gelten muss: $p_a < p_i \leq \sqrt{x}$. Setzen wir jetzt $b := \pi(\sqrt{x})$, und nehmen wir an, dass $a < b$ gilt, dann erhalten wir insgesamt:

$$\begin{aligned} P_2(x,a) &= \sum_{i=a+1}^{b} \left(\pi\left(\frac{x}{p_i}\right) - (i-1)\right) = \\ &= -\frac{(b-a)(b+a-1)}{2} + \sum_{i=a+1}^{b} \pi\left(\frac{x}{p_i}\right). \end{aligned} \tag{3.69}$$

Definiert man abschließend $a = c := \pi\left(x^{\frac{1}{3}}\right)$, um $P_3(x,a)$ und die höheren Summen vernachlässigen zu können, erreicht man Meissel's Formel:

$$\begin{aligned} \pi(x) &= \lfloor x \rfloor - \sum_{i=1}^{c} \left\lfloor \frac{x}{p_i} \right\rfloor + \sum_{1 \leq i < j \leq c} \left\lfloor \frac{x}{p_i p_j} \right\rfloor - \cdots + \\ &\quad + \frac{(b+c-2)(b-c+1)}{2} - \sum_{c < i \leq b} \pi\left(\frac{x}{p_i}\right). \end{aligned} \tag{3.70}$$

### 3.4.3 Verfahren nach Lehmer

Nachdem wir uns jetzt etwas genauer mit $P_2(x,a)$ beschäftigt haben, und dadurch zu Meissel's Formel gestoßen sind, liegt es auf der Hand, mit einer ähnlichen Vorgangsweise zu versuchen, einen Schritt weiter zu kommen, und $P_3(x,a)$ zu analysieren. Tatsächlich ist dies jener Trick, der direkt zur nächsten Verbesserung der ursprünglichen Formel (3.65) führt. Aus diesem Grund wird vorerst auf eine Implementierung in DERIVE verzichtet.

Wieder halten wir je eine der drei Primzahlen fest, die in $P_3(x,a)$ eine Rolle spielen, und gelangen somit zu

$$\begin{aligned} P_3(x,a) &= \text{Anzahl der Zahlen } p_{a+1}p_jp_k \le x \text{ mit } a+1 \le j \le k \\ &\quad + \text{Anzahl der Zahlen } p_{a+2}p_jp_k \le x \text{ mit } a+2 \le j \le k \\ &\quad + \cdots \\ &= P_2\left(\frac{x}{p_{a+1}}, a\right) + P_2\left(\frac{x}{p_{a+2}}, a+1\right) + \cdots \\ &= \sum_{i>a} P_2\left(\frac{x}{p_i}, (i-1)\right). \end{aligned} \tag{3.71}$$

Nun führen wir folgende Größen ein: $b_i := \pi\left(\sqrt{\frac{x}{p_i}}\right)$, sodass sich mit Hilfe von (3.69) ergibt:

$$P_3(x,a) = \sum_{i>a} P_2\left(\frac{x}{p_i}, i-1\right) = \sum_{i=a+1}^{c} \sum_{j=i}^{b_i} \left(\pi\left(\frac{x}{p_ip_j}\right) - (j-1)\right). \tag{3.72}$$

Hierbei wird angenommen, dass $a < c := \pi\left(x^{\frac{1}{3}}\right)$ gilt, um sicher zu stellen, dass $P_3(x,a)$ von Null verschiedene Terme enthält. Setzt man schließlich $a := \pi\left(x^{\frac{1}{4}}\right)$, so hat man die ursprüngliche Formel von D.H.Lehmer erreicht:

$$\begin{aligned} \pi(x) = \lfloor x \rfloor - \sum_{i=1}^{a} \left\lfloor \frac{x}{p_i} \right\rfloor + \sum_{a \le i < j \le a} \left\lfloor \frac{x}{p_ip_j} \right\rfloor - \cdots + \frac{(b+a-2)(b-a+1)}{2} - \\ - \sum_{a<i\le b} \pi\left(\frac{x}{p_i}\right) - \sum_{i=a+1}^{c} \sum_{j=i}^{b_i} \left(\pi\left(\frac{x}{p_ip_j}\right) - (j-1)\right). \end{aligned} \tag{3.73}$$

Bei der tatsächlichen Berechnung von $\pi(x)$ stellt sich heraus, dass den arbeitsintensivsten Teil dieser Rechnungen die sogenannte „Legendre-Summe“ darstellt.

Man versteht darunter folgenden Ausdruck

$$\Phi(x,a) = \lfloor x \rfloor - \sum \left\lfloor \frac{x}{p_i} \right\rfloor + \sum \left\lfloor \frac{x}{p_i p_j} \right\rfloor - \sum \left\lfloor \frac{x}{p_i p_j p_k} \right\rfloor + \cdots , \qquad (3.74)$$

der die Anzahl jener Zahlen $\leq x$ darstellt, die durch keine der ersten $a$ Primzahlen $p_1 = 2, p_2 = 3, \ldots, p_a$ teilbar sind. Angesichts der einfachen Implementierung dieser Funktion in DERIVE scheint diese Tatsache kaum vorstellbar:

```
Phi(x, a) :=
  If a = 0
     FLOOR(x)
     Phi(x, a - 1) - Phi(x/NTH_PRIME(a), a - 1)
```

Bei dieser rekursiven Implementierung macht man sich einen ersten Trick zu Nutze, um die Berechnung von (3.74) möglichst einfach zu gestalten.

Da $\Phi(x,a)$ die Anzahl der Zahlen $\leq x$ bezeichnet, die nicht durch eine der ersten $a$ Primzahlen teilbar sind, kann man $\Phi(x,a)$ auch durch folgende Rekursion definieren:

$$\Phi(x,a) = \Phi(x,a-1) - \Phi\left(\frac{x}{p_a}, a-1\right). \qquad (3.75)$$

Diese Formel besagt eigentlich nur, dass jene Zahlen, die durch keine der ersten $a$ Primzahlen geteilt werden können, genau jene sind, die durch keine der ersten $a-1$ Primzahlen $p_1, \ldots, p_{a-1}$ dividiert werden können, mit Ausnahme der Zahlen, die durch $p_a$ teilbar sind.

Unter Verwendung von (3.75) berechnet man $\Phi(x,a)$ rekursiv bis zu $\Phi(x,1)$ (= Anzahl der ungeraden Zahlen $\leq x$). In unserem Programm gehen wir noch einen Schritt weiter, und berechnen die Legendre-Summe bis $\Phi(x,0)$. Da wir uns jedoch später Weiterentwicklungen zuwenden werden, geben wir uns mit der hier gewählten Vorgangsweise vorläufig zufrieden. Unter Verwendung von `Phi(x,a)` könnte eine zweite Version der Legendre'schen Formel in DERIVE so aussehen

```
legendre(x, l_) :=
  If x < 2
     0
     Prog
       l_ := legendre(SQRT(x))
       l_ + Phi(x, l_) - 1
```

Erinnern wir uns kurz an die vorhergehende Version `leg(x,k)`. Diese benötigte für die Berechnung von $\pi(1.000)$ noch 13.9 Sekunden. Die Wahl eines zweiten Parameters muss bei der neuen Implementierung nicht getroffen werden, und so ergibt sich

`legendre(1000) = 168` (0.561 Sekunden).

Dies ist deutlich schneller als `leg(1000,4)`. Es ist auch möglich, ohne großen Aufwand die Formel nach Meissel zu implementieren:

```
meissel(x, b_, c_) :=
  If x < 2
     0
     Prog
       c_ := meissel(x^(1/3))
       b_ := meissel(SQRT(x))
       Phi(x, c_) + (b_ + c_ -2)(b_ - c_ +1)/2 -
        SUM(meissel(x/NTH_PRIME(n)), n, FLOOR(c_+1), FLOOR(b_))
```

Berechnet man damit die Primzahlen $p \leq 1.000$, so stellt sich abermals ein - wenn auch weit kleinerer - Zeitgewinn ein:

`meissel(1000) = 168` (0.291 Sekunden).

Ein weiterer Vergleichswert für $x = 2.000$

`legendre(2000) = 303` (4.35 Sekunden)
`meissel(2000) = 303` (0.491 Sekunden)

zeigt, wo die Stärken der Meissel'schen Variante liegen. Die Verbesserungen werden erst für größer werdende Werte von $x$ sichtbar. Für kleine $x$, etwa $x = 100$, kann mitunter auch eine Verschlechterung eintreten.

Von einer Programmierung von Lehmer's Variante wird an dieser Stelle abgesehen, zumal sie keinerlei relevante Verbesserung mit sich bringt. Bevor wir uns jedoch mit der nächsten Weiterentwicklung beschäftigen, wollen wir uns noch einmal der Legendre-Summe $\Phi(x, a)$ zuwenden. Auch wenn die Berechnung von $\Phi(x, a)$ mit Hilfe von (3.75) auf die Berechnung von $\Phi(x, 0)$ resp. $\Phi(x, 1)$ zurückzuführen ist, erweist es sich in der Praxis doch als viel besser, einen Weg zu finden, nur bis zu $\Phi(x, k)$ mit einem bestimmten $k$ rechnen zu müssen. Dies kann durch folgende Überlegung erreicht werden:

Man definiert zunächst $m_k := p_1 p_2 \cdots p_k$, und betrachtet Legendre's Formel für $x = m_k$:

$$\begin{aligned}
\Phi(m_k, k) &= \lfloor (m_k) \rfloor - \sum \left\lfloor \frac{m_k}{p_i} \right\rfloor + \sum \left\lfloor \frac{m_k}{p_i p_j} \right\rfloor - \cdots = \\
&= m_k - \sum \frac{m_k}{p_i} + \sum \frac{m_k}{p_i p_j} - \cdots = \\
&= m_k \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) = \\
&= \prod_{i=1}^{k} (p_i - 1) = \varphi(m_k). \qquad (3.76)
\end{aligned}$$

Da alle Quotienten in der ersten Zeile ganzzahlig sind, können ohne Weiteres die Gauss-Klammern weggelassen und diese Vereinfachung vorgenommen werden. (Für die Definition der Euler'schen $\varphi$-Funktion siehe gegebenfalls Definition 1.1.11).

Auf Grund der Periodizität und wegen (3.76) ergibt sich nunmehr

$$\Phi(s \cdot m_k + t, k) = s \cdot \varphi(m_k) + \Phi(t, k), \qquad (3.77)$$

wobei für $t$ gilt: $0 \leq t < m_k$. Weiters kann für $t > \frac{m_k}{2}$ neben der Periodizität auch die Symmetrie der Vielfachen um Null ausgenutzt werden, sodass man schließlich bei

$$\Phi(t, k) = \varphi(m_k) - \Phi(m_k - t - 1, k) \qquad (3.78)$$

landet. Somit wäre eine Tabelle mit Werten von $\Phi(x, k)$ für $0 \leq x < \frac{m_k}{2}$ wünschenswert. Diese kann man in Form einer „kritischen" Tabelle abspeichern, das heißt, es werden nur jene Wertepaare $(x, \Phi(x, k))$ gespeichert, in denen sich $\Phi(x, k)$ ändert.

Um die in DERIVE eingebaute Routine `PRIMEPI(x)` zu verbessern, und eine Berechnung von $\pi(10^{10})$ in vernünftiger Zeit zu erreichen, wollen wir auch diesen Weg nicht weiter verfolgen. Eine Tabelle für $k = 7$ etwa besitzt bereits 47.081 Einträge. Das erfordert wiederum eine effiziente Verarbeitung der Liste, um dem Ziel einen Schritt näher zu kommen.

### 3.4.4 Algorithmus von Mapes

Nachdem die drei vorangegangenen Methoden mehr oder weniger ausgefeilte Varianten einer einzigen Idee waren, wollen wir uns jetzt mit einer 1963 von

David C. Mapes entwickelten, noch besseren Art und Weise, die Terme in der Legendre'sche Summe zu kombinieren, beschäftigen. Dazu ist es zunächst erforderlich, einige Schreibweisen einzuführen. Auf eine Implementierung, bzw. eine Vertiefung in diese eher komplizierte Form der Berechnung von $\pi(x)$ wollen wir wieder verzichten. Der Interessierte sei dazu auf [Rie94] verwiesen, bzw. auf Mapes [Map63] selber.

Zu Beginn steht die Beobachtung, dass die Legendre-Summe

$$\Phi(x,a) = \lfloor x \rfloor - \sum \left\lfloor \frac{x}{p_i} \right\rfloor + \sum \left\lfloor \frac{x}{p_i p_j} \right\rfloor - \sum \left\lfloor \frac{x}{p_i p_j p_k} \right\rfloor + \cdots , \tag{3.79}$$

mit $p_i < p_j < p_l \leq p_a$, und $p_a$ ist die $a$-te Primzahl, aus genau $2^a$ Termen besteht. Dies ermöglicht es, jeden einzelnen dieser $2^a$ Terme folgendermaßen darzustellen:

$$T_k(x,a) = (-1)^{\beta_0+\beta_1+\cdots+\beta_{a-1}} \left\lfloor \frac{x}{p_1^{\beta_0} p_2^{\beta_1} \cdots p_a^{\beta_{a-1}}} \right\rfloor . \tag{3.80}$$

Hierbei sollen unter $\beta_i$ die Stellen in der Binärdarstellung von $k$ verstanden werden (d.h. $\beta_i \in \{0,1\}$):

$$k = 2^{a-1}\beta_{a-1} + 2^{a-2}\beta_{a-2} + \cdots + 2^1\beta_1 + 2^0\beta_0. \tag{3.81}$$

Obwohl diese Schreibweise einen komplizierten Eindruck erweckt, steckt doch nur ein formaler Trick dahinter: Man ordne $2^{n-1}$ die n-te Primzahl $p_n$ zu. Folglich wird 2 als erste Primzahl mit $2^0$ verbunden, 3 mit $2^1$, 5 mit $2^2$ usw. Weiters assoziiere man mit dem Produkt von verschiedenen Primzahlen die Summe der unterschiedlichen, den Primzahlen entsprechenden, Potenzen von 2. Das bedeutet $2 \cdot 7$ ist also $2^0 + 2^3$ zugeordnet. Schließlich versieht man die Terme noch mit (3.79) entsprechenden Vorzeichen, und man erhält genau obige „Codierung".

So kann beispielsweise die Legendre-Summe für $a = 3$ folgendermaßen geschrieben werden:

$$\underbrace{\lfloor x \rfloor}_{T_0(x,3)} - \underbrace{\left\lfloor \frac{x}{p_1} \right\rfloor}_{T_1(x,3)} - \underbrace{\left\lfloor \frac{x}{p_2} \right\rfloor}_{T_2(x,3)} + \underbrace{\left\lfloor \frac{x}{p_1 p_2} \right\rfloor}_{T_3(x,3)} - \underbrace{\left\lfloor \frac{x}{p_3} \right\rfloor}_{T_4(x,3)} + \underbrace{\left\lfloor \frac{x}{p_1 p_3} \right\rfloor}_{T_5(x,3)} + \underbrace{\left\lfloor \frac{x}{p_2 p_3} \right\rfloor}_{T_6(x,3)} - \underbrace{\left\lfloor \frac{x}{p_1 p_2 p_3} \right\rfloor}_{T_7(x,3)} . \tag{3.82}$$

Es folgt unmittelbar

$$\Phi(x,a) = \sum_{k=0}^{2^a-1} T_k(x,a). \tag{3.83}$$

Sei jetzt $M$ eine beliebige natürlich Zahl $< 2^a$, und $2^i$ der gerade Anteil an $M$ (d.h. $2^i \mid M$, aber $2^{i+1} \nmid M$). Dann definieren wir

$$\gamma(M, x, a) := \sum_{k=M}^{M+2^i-1} T_k(x, a), \tag{3.84}$$

und erhalten schließlich

$$\Phi(x, a) = T_0(x, a) + \gamma(2^0, x, a) + \gamma(2^1, x, a) + \cdots + \gamma(2^{a-1}, x, a). \tag{3.85}$$

Definiert man weiters $T_k(-x, a)$ als $-T_k(x, a)$, so ergibt sich unter der Voraussetzung $2^i \mid k$

$$\operatorname{sign} T_k(x, a) = (-1)^{\beta_i + \beta_{i+1} + \cdots + \beta_{a-1}}, \tag{3.86}$$

da die letzten $i$ binären Stellen von $k$ alle gleich Null sind; unter der gleichen Voraussetzung gilt auch

$$|T_k(x, a)| = \left\lfloor \frac{x}{p_{i+1}^{\beta_i} p_{i+2}^{\beta_{i+1}} \cdots p_a^{\beta_{a-1}}} \right\rfloor. \tag{3.87}$$

Setzt man jetzt $T_k(x, a)$ für $x$, und $i$ für $a$ in der Definition von $T_{k'}(x, a)$ ein, erhält man

$$T_{k'}\left(T_k(x, a), i\right) = \operatorname{sign}\left(T_k(x, a)\right) (-1)^{\beta'_0 + \beta'_1 + \cdots + \beta'_{i-1}} \cdot \left( \frac{|T_k(x, a)|}{p_1^{\beta'_0} p_2^{\beta'_1} \cdots p_i^{\beta'_{i-1}}} \right), \tag{3.88}$$

wobei die $\beta'_i$ die Binärstellen von

$$k' = 2^{i-1}\beta'_{i-1} + 2^{i-2}\beta'_{i-2} + \cdots + 2^1\beta'_1 + 2^0\beta'_0 \tag{3.89}$$

sind, und $0 \leq k' < 2^i$ gilt. Angenommen es gelte $2^i \mid k$, so wird (3.88) mit Hilfe von (3.86) und (3.87) zu

$$T_{k'}(T_k(x, a), i) = T_{k+k'}(x, a). \tag{3.90}$$

Aber Achtung: Nur wenn $k$ und $k'$ die Einser in ihrer Binärdarstellung an unterschiedlichen Stellen haben, können sie in einer mit der Definition (3.80) in Einklang stehenden Art und Weise addiert werden, ohne dass dabei ein Überlauf auftritt. Daraus resultieren die beiden Einschränkungen $k' < 2^i$ und $2^i \mid k$.

Setzt man jetzt $T_M(x,a)$ für $x$ und gleichzeitig $i$ für $a$ in der Legendre-Summe (3.79), so erhält man

$$\Phi(T_M(x,a),i) = \sum_{k'=0}^{2^i-1} T_{k'}(T_M(x,a)) = \sum_{k=M}^{M+2^i-1} T_k(x,a) = \gamma(M,x,a). \quad (3.91)$$

Nunmehr kann die Summe $\Phi(x,a)$ in (3.85) mit dieser Notation in folgender Weise umgeschrieben werden

$$\Phi(x,a) = T_0(x,a) + \Phi(T_1(x,a),0) + \Phi(T_2(x,a),1) + \cdots + \Phi(T_{2^a-1}(x,a),a-1). \quad (3.92)$$

Wenn wir abermals $x$ mit $T_M(x,a)$ und gleichzeitig $a$ mit $i$ in (3.92) ersetzen, bekommen wir unter Verwendung von (3.90):

$$\begin{aligned} &\Phi(T_M(x,a),i) = T_0(T_M(x,a),i) + \Phi(T_1(T_M(x,a),i),0) + \\ &+\Phi(T_2(T_M(x,a),i),1) + \cdots + \Phi(T_{2^{i-1}}(T_M(x,a),i),i-1) = \\ &= T_M(x,a) + \Phi(T_{M+1}(x,a),0) + \Phi(T_{M+2}(x,a),1) + \cdots + \\ &\quad +\Phi(T_{M+2^r}(x,a),r) + \cdots + \Phi(T_{M+2^{i-1}}(x,a),i-1), \end{aligned} \quad (3.93)$$

falls $2^i \mid M$ gilt. (Man beachte, dass nach (3.83) folgt: $\Phi(T_{M+1}(x,a),0) = T_{M+1}(x,a)$.)

Beginnend mit $\Phi(x,a) = \Phi(T_0(x,a),a)$ kann jetzt (3.93) $\Phi(x,a)$ rekursiv berechnet werden. Auch diesmal ist es hilfreich, wenn für kleine $a$ entsprechende Tabellen für $\Phi(x,a)$ zur Verfügung stehen. Weiters empfiehlt sich bei der Berechnung von $\Phi(x,a)$ die Verwendung von (3.77) bzw. von (3.78).

Wie schon zu Beginn dieses Abschnittes erklärt, wird hier sowohl auf eine Umsetzung der Theorie in DERIVE, als auch auf ein Rechenbeispiel verzichtet. Einzig der Hinweis, dass ein solches etwa in [Rie94] zu finden ist, sei an dieser Stelle noch hinzugefügt.

### 3.4.5 Neuere Entwicklungen

Nach dem Exkurs in die etwas komplizierte Begriffswelt von Mapes wollen wir uns jetzt noch kurz weiteren Methoden zur Berechnung von $\pi(x)$ widmen, ehe wir im Detail jene Funktionen untersuchen, die es in DERIVE schließlich möglich machen, $\pi(10^9)$ bzw. $\pi(10^{10})$ zu berechnen.

Zuerst sei hier eine kombinatorische Methode nach Lagarias, Miller und Odlyzko erwähnt, deren Wurzeln unter anderem auch in den Arbeiten von

Meissel und Lehmer zu finden sind. Nebenbei bemerkt wurde eine Version genau dieses Algorithmusses in MATHEMATICA implementiert, um dort die Funktion $\pi(x)$ zu berechnen.

Die Originalarbeit findet man unter [LMO85], eine Weiterentwicklung etwa in [DR96]. Der große Fortschritt bei dieser Methode liegt zweifellos in einer weiteren Verbesserung der Rechenzeit und des Speicherbedarfs. Das Hauptaugenmerk bei einer detaillierten Besprechung der folgenden Algorithmen müsste wohl auf den Nachweis, dass man wirklich mit einem Aufwand von $O(x^{\frac{2}{3}+\epsilon})$ an Operationen und einem Speicherbedarf der Ordnung $O(x^{\frac{1}{3}+\epsilon})$ auskommt, gelegt werden. Da dafür eine umfassende Analyse erforderlich wäre, wollen wir hier darauf verzichten. Der Interessierte sei auf die Originalarbeiten oder z.B. auch auf [CP01] verwiesen.

Zu Beginn der Beobachtungen steht folgende Identität, die man leicht selbst überprüfen kann:

$$\Phi(x,a) = P_0(x,a) + P_1(x,a) + P_2(x,a) + \cdots , \tag{3.94}$$

wobei $P_0(x,a) = 1$ gilt für $x \geq 1$. Wie wir uns im Zusammenhang mit Formel (3.67) bereits überlegt haben, gilt $P_k(x,a) = 0$ für $p_a^k \geq x$, sodass auch folgendes erfüllt ist:

$$\Phi(x,\pi(x^{1/3})) = 1 + \pi(x) - \pi(x^{1/3}) + P_2(x,\pi(x^{1/3})). \tag{3.95}$$

Dies ist die Gleichung, mit deren Hilfe im Verfahren nach Lagarias, Miller und Odlyzko $\pi(x)$ bestimmt wird. Es ist offensichtlich, dass man $\pi(x)$ unter Kenntnis von $\Phi(x,\pi(x^{1/3})), P_2(x,\pi(x^{1/3}))$ und $\pi(x^{1/3})$ leicht berechnen kann. Letzteres wird dabei durch ein simples Siebverfahren ermittelt. Die nächsteinfachere unbekannte Größe ist $P_2(x,\pi(x^{1/3}))$, deren Bestimmung im Folgenden beschrieben wird. Es gilt:

$$P_2(x,\pi(x^{1/3})) = \tbinom{\pi(x^{1/3})}{2} - \tbinom{\pi(x^{1/2})}{2} + \sum_{\pi(x^{1/3})<i\leq\pi(x^{1/2})} \pi\left(\frac{x}{p_i}\right). \tag{3.96}$$

Diese Beziehung gilt ganz analog zu (3.69), nur dass wir hier nicht die herkömmliche Summenformel für eine arithmetische Reihe verwenden, sondern:

$$\begin{aligned} \sum_{\pi(x^{1/3})<i\leq\pi(x^{1/2})} (i-1) &= \sum_{i=1}^{\pi(x^{1/2})} (i-1) - \sum_{i=1}^{\pi(x^{1/3})} (i-1) \\ &= \tbinom{\pi(x^{1/2})}{2} - \tbinom{\pi(x^{1/3})}{2}, \end{aligned} \tag{3.97}$$

womit (3.96) bewiesen wäre.

Um (3.96) verwenden zu können, benötigen wir also $\pi(x^{1/3}), \pi(x^{1/2})$ und die Summe der $\pi(x/p_i)$. Die erste Größe haben wir bereits berechnet und $\pi(x^{1/2})$ wird ebenfalls mit Hilfe eines Siebes ermittelt, nur mit dem Unterschied, dass es auf Blöcke von ungefähr der Länge $x^{1/3}$ zerteilt wird. Nachdem in der Summe in (3.96) für jeden Summanden $\frac{x}{p}$ gilt:

$$\frac{x}{p} < x^{2/3} \tag{3.98}$$

kann man sie abermals durch ein simples Sieb nach Eratosthenes in einer Zeit von $O(x^{2/3+\epsilon})$ berechnen. Bei entsprechender Vorgangsweise kommt man mit einem Speicherbedarf von $O(x^{1/3+\epsilon})$ aus.

Wir wenden uns zum Abschluss noch der ausstehenden Größe $\Phi(x, \pi(x^{1/3}))$ zu. Der Trick dabei ist wieder, die Berechnung von $\Phi(x, \pi(x^{1/3}))$ auf jene von viel kleineren Problemen zu reduzieren, wie das etwa mit der Rekursion (3.75) geschehen kann. Durch ständiges Anwenden dieser Beziehung gelangt man schließlich zu einer Gleichung der Form:

$$\Phi(x,a) = \sum_{n|p_1p_2\cdots p_a} \mu(n)\Phi(x/n) = \sum_{n|p_1p_2\cdots p_a} \mu(n) \left\lfloor \frac{x}{n} \right\rfloor, \tag{3.99}$$

wobei $\mu$ die Möbius'sche $\mu$-Funktion ist. Auch wenn wir uns folgende Identität zu Nutze machen: $\Phi(x,1) = \lfloor (x+1)/2 \rfloor$, so sind die verbleibenden $2^{a-1}$ Terme viel zu viele, als dass dieser Rechenweg interessant wäre. Wir müssen jedoch nicht jedes $n$ in Betracht ziehen mit $n \mid p_2p_3\cdots p_a$, da für $n > x$ natürlich $\Phi(x/n, 1) = 0$ gilt. Diese Abbruchbedingung reduziert die Anzahl der Terme auf ein $O(x)$, was langsam mit Siebmethoden vergleichbar wird.

Da $m_5 = p_1p_2\cdots p_5 = 2.310$ gilt, könnte man etwa unter Verwendung von (3.77) und einer Tabelle mit Werten von $\Phi(x,5)$ für alle $x = 0, 1, \ldots, 2.309$, für beliebiges $x$ den Wert von $\Phi(x,5)$ sehr rasch berechnen. Bricht man jetzt die Rekursion (3.75) jeweils dann ab, wenn $a = 5$, oder $x/p_a < 1$ gilt, so erhält man

$$\Phi(x,a) = \sum_{n|p_6p_7\cdots p_a, n\le x} \mu(n)\Phi(x/n, 5). \tag{3.100}$$

Nachwievor gilt $a = \pi(x^{1/3})$, sodass sich die Anzahl der in (3.100) auftretenden Summanden asymptotisch zu $cx$ ergibt, mit

$$c = \rho(3)\zeta(2)^{-1} \prod_{i=1}^{5} \frac{p_i}{p_i+1}, \tag{3.101}$$

wobei $\rho$ die Dickman-Funktion (siehe Satz 1.1.13) und $\zeta$ die Riemann'sche $\zeta$-Funktion ist. Setzt man $\rho(3) \approx 0.0486$ und $\zeta(2)^{-1} = \frac{6}{\pi^2}$ ein, so ergibt sich $c \approx 0.00987$.

Da der vorliegende Algorithmus jedoch nur $O(x^{2/3+\epsilon})$ Zeit benötigen will, muss er sich einer anderen Abbruchbedingung bedienen. Er bricht die Rekursion (3.75) von $\Phi(y, b)$ immer dann ab, wenn einer der beiden Fälle erfüllt ist:

1. $b = 1$ und $y \geq x^{2/3}$
2. $y < x^{2/3}$

Dabei hat $y$ die Form $x/n$, wo $n \mid p_2 p_3 \cdots p_a$ gilt. Wieder lassen sich durch geschickte Rechenschritte die angepeilten Aufwandsgrenzen erreichen. V.S. Miller hat diesen Algorithmus auch implementiert, wenngleich er dazu einige Modifikationen der theoretischen Form des Verfahrens vornehmen musste. Es gelang ihm damit, den Wert von $\pi(10^{13})$ aus der Tabelle von Jan Bohman zu korrigieren. Bohman erreichte in seinem Artikel [Boh72], in dem er eine Methode nach Mapes verwendete, einen um 941 zu geringen Wert für $\pi(10^{13})$. Darüberhinaus berechnete Miller verschiedene Werte bis $4 \cdot 10^{16}$.

Neben diesem Algorithmus wird in [LMO85] noch eine Erweiterung davon beschrieben, die auf $M \leq x^{1/3}$ verschiedenen Prozessoren parallel rechnet. Die dabei entstehende Komplexität wird mit einem Zeitaufwand von $O(M^{-1}x^{2/3+\epsilon})$ und einem Speicherbedarf von $O(x^{1/3+\epsilon})$ pro Prozessor, also $O(Mx^{1/3+\epsilon})$ insgesamt, angegeben. Ideen zur Weiterentwicklung des Algorithmus findet man auch in [DR98].

Zum Abschluss soll an dieser Stelle noch ein weiterer Algorithmus zur Berechnung von $\pi(x)$ erwähnt werden. In [LO87] beschreiben hiezu Lagarias und Odlyzko eine analytische Methode. Bisher ist jedoch die kombinatorische noch überlegen, sodass es keine praktischen Resultate für den analytischen Algorithmus gibt. Das dürfte aber nur eine Frage der Zeit sein; bisher hält man erst Werte von $10^{13}$ bis höchstens $10^{14}$ für damit erreichbar. Einen kurzen Abriss dieses Verfahrens findet man in [CP01].

### 3.4.6 Implementierung in DERIVE

Zunächst werden noch einmal die Größen $P_k(x, a)$ analysiert. Sie bezeichnen bekanntlich die Anzahl der Zahlen $\leq x$, die das Produkt von genau $k$ (nicht notwendigerweise verschiedener) Primzahlen $> p_a$ sind. Es gilt offenbar

$$P_1(x,a) = \max(\pi(x) - a, 0) \tag{3.102}$$

$$P_k(x,a) = P_{k-1}\left(\frac{x}{p_{a+1}}, a\right) + \cdots + P_{k-1}\left(\frac{x}{p_{a+m}}, a+m-1\right) \tag{3.103}$$

wobei $m$ die größte natürliche Zahl mit $p_{a+m}^k \leq x$ ist. (Man kann ja

$$P_{k-1}\left(\frac{x}{p_{a+j}}, a+j-1\right), 1 \leq j \leq m \tag{3.104}$$

als Anzahl aller Zahlen $\leq x$ interpretieren, die genau $k$ Primfaktoren $\geq p_{a+j}$ haben.)

Wenn wir uns an (3.67) erinnern, so gilt

$$\pi(x) = \Phi(x,a) + a - 1 - P_2(x,a) - P_3(x,a) - \cdots - P_{m-1}(x,a) \tag{3.105}$$

mit $p_{a+1}^{m-1} \leq x < p_{a+1}^m$. Um diese letzte Bedingung sicherzustellen, kann man etwa $a = \pi(\sqrt[m]{x})$ wählen. Unser Grundgedanke besteht nun darin, für kleine Werte durch ein Netz von Stützstellen, an denen die dazugehörigen Funktionswerte von $\pi(x)$ gespeichert wurden, durch einfaches Abzählen von der nächstgelegenen Stützstelle weg den tatsächlichen Wert von $\pi(x)$ zu bestimmen. Im vorliegenden Fall wird ein Netz für $x \leq 10^7$ angelegt, und darüber hinaus mittels (3.105) weitergerechnet.

Im Folgenden werden weitgehend Funktionsnamen, wie sie durch [Wie97] vorgegeben sind, verwendet. Zunächst wenden wir uns der Erstellung der Tabellen zu. Dafür benötigen wir ein Programm, das die Anzahl der Primzahlen $p$ mit $s < p \leq x$ berechnet, etwa:

```
ppi(x, s, k_ := -1, p_) :=
  Prog
    p_ := s
    Loop
      If p_ > x
         RETURN k_
      p_ := NEXT_PRIME(p_)
      k_ :+ 1
```

Mit Hilfe von `ppi(x,s)` werden 4 Listen mit unterschiedlichen Zahlenbereichen und Schrittweiten angefertigt; sie sollen für eine Primzahltabelle bis $10^7$ dienen:

Zunächst wird eine Liste für $7 \leq x \leq 1.002$ erstellet. Dazu speichern wir $\pi(x)$ nur für die Werte von $x$, die nicht durch eine der ersten 3 Primzahlen $2, 3, 5$ teilbar sind:

```
INSERT(0,VECTOR(ppi(x_,0),x_,SELECT(GCD(k_,30)=1,k_,7,1001)))
```

Weiter geht es mit $1.002 < x < 100.100$, und einer Schrittweite von 100:

```
Prog(
  s_ := ppi(1000,0)
  v_ := [s_]
  x_ := 1000
  Loop
    s_ :+ ppi(x_ + 100, x_)
    v_ := INSERT(s_, v_)
    x_ :+ 100
    If x_ = 100000
       RETURN REVERSE(v_)
```

Ganz analog werden Tabellen für $100.099 < x < 1.000.500$ - mit einer Schrittweite von 500 - und $1.000.499 < x < 10.010.000$, in Schritten von 10.000, angelegt. (Die entsprechenden Werte sind einfach in der obigen Programmstruktur zu ersetzen.)

Bevor wir die somit erhaltenen Tabellen in unseren Programmablauf einbauen können, müssen wir uns die Routinen schreiben, die zwischen den Stützstellen interpolieren. Dabei wird, je nachdem ob wir der oberen Grenze oder der unteren näher sind, von oben heruntergezählt, oder von unten hinauf. Zum Runterzählen wird zu allererst ein Pendant zur eingebauten Routine `NEXT_PRIME` benötigt:

```
prev_prime(x) :=
  If PRIME(x - 1)
     x - 1
     prev_prime(x - 1)
```

Schließlich zählt `ip1(x,p,s)` die Primzahlen von $p$ bis $x$ zur Zahl $s$ hinzu, wobei hinaufgezählt wird

```
ip1(x, p, s) :=
  If p > x
     s
     ip1(x, NEXT_PRIME(p), s + 1)
```

`ip2(x,p,s)` zählt analog in die entgegengesetzte Richtung von $x$ nach $p$ hinunter

```
ip2(x, p, s) :=
  If p <= x
     s
     ip2(x, prev_prime(p), s-1)
```

Mit `ip(x,d,o,l)` wird der echte Wert von $\pi(x)$ zwischen den Stützstellen mit der Schrittweite $d$ interpoliert. $o$ wird dabei zum richtigen Ansteuern der Liste $l$ verwendet.

```
ip(x, d, o, l) :=
  If MOD(x, d) < 3d/5
     ip1(x, NEXT_PRIME(FLOOR(x, d)d), lSUB(FLOOR(x, d) - o))
     ip2(x, prev_prime((FLOOR(x, d)+1)d), lSUB(FLOOR(x,d)-o+1))
```

Im Folgenden sind die 4 Routinen notiert, die den Wert für $\pi(x)$ unter Verwendung der entsprechenden Listen zurückgeben. Diese sind dabei jeweils nur angedeutet:

```
pit(x) :=
  If x < 7
     [0, 1, 2, 2, 3, 3]SUBFLOOR(x)
     [0, 4, 5, 6, 7, ..., 166, 167, 168, 168]SUB(-FLOOR(x/30)
       + FLOOR(x/15) + FLOOR(x/10) + FLOOR(x/6) - FLOOR(x/5)
       - FLOOR(x/3) - FLOOR(x/2) + FLOOR(x))

piht(x) := ip(x, 100, 9, [168, 184, 196, ..., 9584, 9592])

pim(x) := ip(x, 500, 199, [9592, 9632, 9673,..., 78466, 78498])

pizm(x) := ip(x, 10000, 99, [78498, 79251,..., 663965, 664579])
```

Somit ergibt sich $\pi(x)$ für alle $x < 10^7 + 9.999$ zu

```
smallpi(x) :=
  If x < 1001
     pit(x)
     If x < 100060
        piht(x)
        If x < 1000000
           pim(x)
           pizm(x)
```

Da wir im Folgenden eine Methode `primepi` benötigen, setzen wir sie der Einfachheit halber zunächst mit `smallpi` gleich:

```
primepi(x) := smallpi(x)
```

Bei der kommenden Funktion wird aus Rechenzeitgründen der alten Implementierung, wie sie in DERIVE 4 vorgenommen wurde, der Vorzug gegeben. `sel(x,k,a)` ermittelt jene Primzahlen, die bei er Berechnung von $P_k(x,a)$ benötigt werden:

```
sel(x, k, a) := DELETE_ELEMENT(ITERATES(NEXT_PRIME(p_), p_,
  ITERATE(NEXT_PRIME(q_), q_, 1, a), MAX(primepi(x^(1/k)-a,0)))
```

Somit können wir $P_k(x,a)$ mittels

```
P(x, k, a, s_) :=
  Prog
    s_ := sel(x, k, a)
    If k = 2
       RETURN -DIM(s_)(DIM(s_)+2a-1)/2 + SUM(primepi(x/t_,t_,s_)
    SUM(P(FLOOR(x/u_), k - 1, smallpi(u_) - 1), u_, s_)
```

berechnen. Hält man sich an dieser Stelle (3.105) vor Augen, so ist der hintere Teil der Formel erledigt. Es bleibt im Wesentlichen „nur“ mehr die Berechnung von $\Phi(x,a)$ zu implementieren. Eine Möglichkeit wurde bereits präsentiert, bzw. eine rudimentäre Realisation in DERIVE vorgestellt. Diesmal wollen wir aber mehr ins Detail gehen und rechnen nicht bis $a = 0$ zurück, sondern überlegen uns, ausgehend von (3.75) folgendes:

$$\begin{aligned}
\Phi(x,a) &= \Phi(x,a-1) - \Phi\left(\frac{x}{p_a}, a-1\right) = \\
&= \Phi(x,a-2) - \Phi\left(\frac{x}{p_{a-1}}, a-2\right) - \Phi\left(\frac{x}{p_a}, a-1\right) = \\
&= \Phi(x,a-3) - \Phi\left(\frac{x}{p_{a-2}}, a-3\right) - \Phi\left(\frac{x}{p_{a-1}}, a-2\right) \\
&\quad -\Phi\left(\frac{x}{p_a}, a-1\right) = \cdots \\
&= \Phi(x,k) - \sum_{i=k+1}^{a} \Phi\left(\frac{x}{p_i}, i-1\right). \qquad (3.106)
\end{aligned}$$

In dem konkreten Fall wird $k = 10$ gesetzt, und dafür $\Phi(x,10)$ in `f10(x)` abgespeichert:

```
f10(x) := FLOOR(x/6469693230) - FLOOR(x/3234846615) - ... -
          - FLOOR(x/3) - FLOOR(x/2) + FLOOR(x)
```

Die benötigten Routinen, um diese Programmierung zu automatisieren, sollen an dieser Stelle nicht besprochen werden. Die Implementierung von $\Phi(x, a)$ ergibt sich somit zu

```
ff(x, a) :=
  If x < 10009999 AND a >= smallpi(SQRT(x))
     MAX(smallpi(x) + 1 - a, 0)
     f10(x) - SUM(ff(x/NTH_PRIME(a_), a_ - 1), a_ , 11, a)
```

Dabei ist die auftauchende Funktion `NTH_PRIME` durch

```
NTH_PRIME(n) := ITERATE(NEXT_PRIME(p_), p_, 1, n)
```

definiert. Somit kann das endgültige Programm, welches die Anzahl der Primzahlen $\leq x$ nach (3.105) berechnet, wie folgt formuliert werden:

```
primepi(x) :=
  If x < 10009999
     smallpi(x)
     ff(x, 15) + 14 - SUM(P(x, i_, 15), i_, 2, 10)
```

Die dabei verwendeten Werte von $a = 15$ und $m = 10$ sind willkürlich gewählt, stellen aber in dieser Form alle nötigen Vorraussetzungen sicher. Mit Hilfe dieses Programmes konnte die Tabelle 3.3 angefertigt werden.

| $x$ | $\pi(x)$ | Zeit |
|---|---|---|
| $10^7$ | 664.579 | 0.00s |
| $2 \cdot 10^7$ | 1.270.607 | 3.34s |
| $5 \cdot 10^7$ | 3.001.134 | 7.17s |
| $10^8$ | 5.761.455 | 14.7s |
| $2 \cdot 10^8$ | 11.078.937 | 26.7s |
| $5 \cdot 10^8$ | 26.355.867 | 61.4s |
| $10^9$ | 50.847.534 | 135.5s |
| $2 \cdot 10^9$ | 98.222.287 | 280.9s |
| $5 \cdot 10^9$ | 234.954.223 | 740.4s |
| $10^{10}$ | 455.052.511 | 1567.3s |

Tabelle 3.3: `primepi(x)` für ausgewählte Werte von $10^7 \leq x \leq 10^{10}$

Mit entsprechendem Programmier-Aufwand ist es somit selbst in nicht auf die Zahlentheorie spezialisierten Computeralgebrasystemen wie DERIVE möglich, die Funktion $\pi(x)$ auf einem herkömmlichen PC für relativ große Werte von $x$ in vernünftiger Zeit zu berechnen.

Die Tatsache, dass wir diese Funktion auch für größere Werte von $x$ rasch auswerten können, ermöglicht es uns umgehend, die Funktion `nth_prime(n)` neu zu implementieren, und somit zu beschleunigen.

Dabei wird so vorgegangen, dass man zunächst für die $n$te Primzahl gemäß (2.108) eine untere Abschätzung $\tilde{n}$ annimmt. Danach wird $\pi(\tilde{n})$ berechnet (in der Regel gilt: $\pi(\tilde{n}) < n$). Davon ausgehend gelangt man iterativ mit `next_prime` bis zum gewünschten $n$.

Die Implementierung kann demnach folgendermaßen aussehen:

```
nprime(n, n_, p_) :=
  Prog
    p_ := FLOOR(n(LN(n) + LN(LN(n)) - 1))
    n_ := primepi(p_)
    ITERATE(NEXT_PRIME(q_), q_, p_, n - n_)
```

Dass das neue Programm zu den gleichen Ergebnissen kommt, wie die eingebaute Version, lässt sich leicht mittels mehrerer willkürlicher Testaufrufe verifizieren. Bemerkenswert ist der Gewinn an Zeit, der mit der neuen Funktion `nprime(n)` einhergeht.

So benötigte `NTH_PRIME(n)` für $n = 10^5$ etwa 20 Sekunden um zu dem Ergebnis

$$p_{100.000} = 1.299.709 \tag{3.107}$$

zu gelangen, verglichen mit etwa 0.3 Sekunden von `nprime(n)`.

# Kapitel 4

# Primzahlen in arithmetischen Folgen

## 4.1 Die erweiterte Riemann'sche Vermutung

Im vorangegangenen Kapitel wurde unter anderem versucht, den Einfluss der Riemann'schen $\zeta$-Funktion und ihrer Nullstellen auf die Verteilung der Primzahlen aufzuzeigen. Dabei stellte sich heraus, dass man - um etwa den Primzahlsatz zu beweisen - die Lage der komplexwertigen Nullstellen von

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} \tag{4.1}$$

genau untersuchen muss. Die Riemann'schen Vermutung 3.1.3 sagt aus, dass jede dieser komplexen Nullstellen von $\zeta(s)$ (im kritischen Streifen) auf der Mittelgeraden $\mathrm{Re}(s) = \frac{1}{2}$ liegt.

Wir wollen uns im Folgenden mit Primzahlen in arithmetischen Folgen auseinandersetzen, und werden dabei zu Beginn eine Erweiterung der obigen Aussage über die Nullstellen von $\zeta(s)$ kennen lernen, die für Fragestellungen bezüglich der Anzahl von Primzahlen in arithmetischen Folgen von entscheidender Bedeutung sein wird.

Doch zunächst müssen einige Begriffe eingeführt werden, um diese Vermutung formulieren zu können. Allen voran lernen wir eine spezielle Art von zahlentheoretischen Funktionen kennen, die sogenannten „Charaktere“:

**Definition 4.1.1** *Es sei $k$ eine natürliche Zahl. Die zahlentheoretische Funktion $\chi(a)$ heißt ein* Charakter *mod $k$, wenn folgende vier Eigenschaften erfüllt sind:*

1. $\chi(a) = 0$ *wenn* $(a, k) \neq 1$
2. $\chi(1) \neq 0$
3. $\chi(ab) = \chi(a)\chi(b)$
4. $\chi(a) = \chi(b)$ *wenn* $a \equiv b(k)$.

*Der durch* $\chi_1(a) = 1$ *für alle zu* $k$ *teilerfremden* $a$ *erklärte Charakter* $\chi_1$ *heißt* Hauptcharakter *mod* $k$.

**Bemerkung 4.1.2** *Für* $\chi$ *gilt darüberhinaus* $\chi : \mathbb{N} \to \mathbb{C}, |\chi(n)| \in \{0, 1\}$. *Weiters sei hier noch die Haupteigenschaft der Charaktere angeschrieben, nämlich*

$$\sum_{l \bmod k} \chi(l) = \begin{cases} \varphi(k) & \chi = \chi_1 \\ 0 & \chi \neq \chi_1 \end{cases} \tag{4.2}$$

Da wir auch hier keinen Beweis des entsprechenden Satzes bringen können, wollen wir nicht weiter in die Theorie der Charaktere eindringen, und es vorderhand bei der Definition belassen. Manchmal werden diese Funktionen auch „Dirichlet'sche Charaktere" genannt.

Vom Aufbau ganz ähnlich zur Riemann'schen $\zeta$-Funktion sind nun die sogenannten „Dirichlet'schen L-Reihen", die gewissermaßen das Pendant dazu in der Theorie der arithmetischen Progressionen bilden. Sie sind folgendermaßen definiert:

**Definition 4.1.3** *Sei* $\chi(n)$ *ein Dirichlet'scher Charakter, dann heißt die dazugehörige Funktion*

$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s} \qquad \mathrm{Re}(s) > 1 \tag{4.3}$$

Dirichlet'sche L-Reihe *zum Charakter* $\chi$. *Die Reihe ist wegen* $|\chi(n)| = 1$ *oder* $0$ *jedenfalls für* $\mathrm{Re}(s) = \sigma > 1$ *konvergent und definiert dort eine analytische Funktion. Insbesondere für* $k = 1$ *gibt es nur den Hauptcharakter, und* $L(s, \chi)$ *geht in* $\zeta(s)$ *über.*

Die Funktion $L(s, \chi)$ besitzt wieder unendlich viele Nullstellen im kritischen Streifen $0 < \mathrm{Re}(s) < 1$. Somit liegt die Erweiterung von 3.1.3 schon so gut wie auf der Hand:

**Vermutung 4.1.4 (Erweiterte Riemann'sche Vermutung)** *Die unendlich vielen komplexwertigen Nullstellen der Dirichlet'schen L-Reihe $L(s,\chi)$ im kritischen Streifen $0 < \mathrm{Re}(s) < 1$ liegen alle auf der Mittelgeraden $\mathrm{Re}(s) = \frac{1}{2}$.*

Ähnlich der ursprünglichen Vermutung 3.1.3 besitzt auch diese erweiterte Form viele Anwendungen und Folgerungen. Einige sind beispielsweise bei [BS96] zu finden; wir wenden uns dem großen Resultat dieses Kapitels zu, in dessen Zusammenhang auch 4.1.4 benötigt wird.

## 4.2 Der Satz von Dirichlet

Man betrachtet zunächst die Verteilung der Primzahlen auf die $\varphi(n)$ primen Restklassen mod $n$. Beispielsweise teilen sich die ersten 1229 Primzahlen $\leq 10^4$ wie folgt auf die beiden Restklassen mod 3 auf: 611 sind $\equiv 1(3)$ und 617 Primzahlen sind $\equiv 2(3)$. So gelangt man schließlich zur

**Definition 4.2.1** *Seien $x$ eine beliebige Zahl, $n$ und $a$ zwei beliebige natürliche Zahlen, dann versteht man unter $\pi_{n,a}(x)$ die Anzahl der Primzahlen $p \leq x$, für die $p \equiv a(n)$ gilt.*

Ähnliche Untersuchungen wie für $\pi_{3,1}(10^4)$ bzw. $\pi_{3,2}(10^4)$ kann man auch für größere Zahlenbereiche, bzw. andere Module vornehmen. DERIVE stellt diesbezüglich die eingebaute Routine `primepi(x,n,a)` zur Verfügung, welche die Anzahl der zu $a$ kongruenten Primzahlen $\leq x$ ausgibt.

| $x$ | $\pi_{3,1}(x)$ | $\pi_{3,2}(x)$ | $\pi_{4,1}(x)$ | $\pi_{4,3}(x)$ |
|---|---|---|---|---|
| $10^2$ | 11 | 13 | 11 | 13 |
| $10^3$ | 80 | 87 | 80 | 87 |
| $10^4$ | 611 | 617 | 609 | 619 |
| $10^5$ | 4.784 | 4.807 | 4.783 | 4.808 |
| $10^6$ | 39.321 | 39.266 | 39.175 | 39.322 |

Tabelle 4.1: $\pi_{3,1}(x)$ versus $\pi_{3,2}(x)$, bzw. $\pi_{4,1}(x)$ versus $\pi_{4,3}(x)$ für jeweils $100 < x < 10^6$.

Wirft man einen Blick auf diese Tabelle, so kann der Eindruck entstehen, dass eine der beiden Funktionen stets größer der anderen ist, dass also jeweils eine der beiden Restklassen mod 3 bzw. 4 stärker besetzt ist als die andere. Tatsächlich verhält es sich dabei genauso wie mit der Funktion $\pi(x)$ und dem

Integrallogarithmus $\mathrm{li}(x)$, die sich bekanntlich unendlich oft an der Spitze abwechseln. Wieder geht das entsprechende Resultat auf Littlewood zurück, der gezeigt hat, dass sich die vermeintlichen Ungleichungen $\pi_{3,1}(x) < \pi_{3,2}(x)$ und $\pi_{4,1}(x) < \pi_{4,3}(x)$ unendlich oft umkehren. Für den Modul 4 gilt etwa (vgl. [Rie94]):

$$\pi_{4,1}(x) - \pi_{4,3}(x) = \Omega\left(\frac{\sqrt{x}\ln\ln\ln x}{\ln x}\right). \tag{4.4}$$

Man weiß also, dass $x$ existieren, für die

$$\pi_{4,3}(x) < \pi_{4,1}(x) \tag{4.5}$$

bzw.

$$\pi_{3,2}(x) < \pi_{3,1}(x) \tag{4.6}$$

gilt. Beim ersten Modul (4) ist ein Beispiel dafür relativ rasch gefunden. Zum ersten Mal wird (4.5) für $x = 26.861$ erfüllt. Dabei gilt $\pi_{4,3}(26.861) - \pi_{4,1}(26.861) = -1$, was wenig spektakulär erscheint. Bei der sechsten „Region“, bei der (4.5) gilt, wird bereits ein Wert von $-2.719$ erreicht, und die Ungleichung ist für immerhin mehr als 410 Millionen aufeinanderfolgender Werte von $x$ erfüllt: $18.54 \cdot 10^9 - 18.95 \cdot 10^9$. Der Grund für diese ungefähre Angabe der Grenzen ist unter anderem auch, dass die genaue Lage noch nicht bekannt ist. In den Abbildungen 4.1 und 4.2 ist die Funktion $\pi_{4,3}(x) - \pi_{4,1}(x)$ aufgezeichnet, um einen kleinen Eindruck zu gewinnen, wie deren Verlauf aussieht.

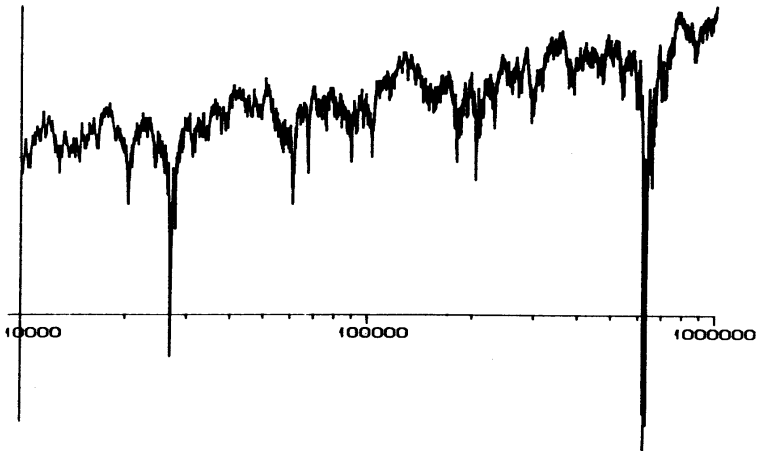


Abbildung 4.1: $\pi_{4,3}(x) - \pi_{4,1}(x)$ für $10^4 \leq x \leq 10^6$.

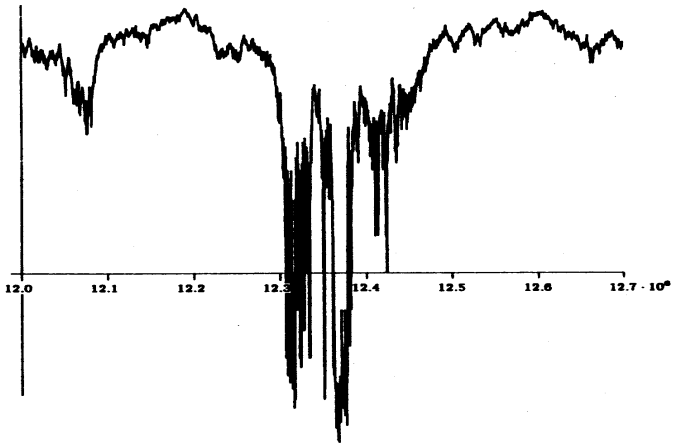


Abbildung 4.2: $\pi_{4,3}(x) - \pi_{4,1}(x)$ für $12 \cdot 10^6 \leq x \leq 12.7 \cdot 10^6$.

Für diesbezügliche weitere Informationen sehe man in [Rie94], [BH78b] bzw. [BH78a] nach.

Vor gut 200 Jahren formulierte Legendre eine Vermutung die Anzahl der Primzahlen in den einzelnen Restklassen betreffen. Sie konnte 1837 erstmals bewiesen werden - die Rede ist vom berühmten Dirichlet'schen Primzahlsatz:

**Satz 4.2.2 (Dirichlet'scher Primzahlsatz)** *Sei $n$ eine beliebige natürliche Zahl, und sei $a$ mit $(a, n) = 1$ ebenfalls beliebig, dann gibt es unendlich viele Primzahlen $p$ mit $p \equiv a(n)$.*

Dass die Forderung $(a, n) = 1$ nicht weggelassen werden kann ist klar, da ansonsten jede Zahl in der Folge $a, a + n, a + 2n, \ldots$ durch den $\mathrm{ggT}(a, n)$ teilbar, also maximal 1 Primzahl in der Folge enthalten wäre.

Wir können auch diesen Satz nicht in dieser allgemeinen Form beweisen, jedoch werden wir zum Abschluss dieses Abschnittes 2 Sonderfälle zeigen. Wenn die Primzahlen gleichverteilt mod $n$ sind, dann sollte die Summe der Primzahlen in einer Kongruenzklasse etwa gleich der entsprechenden Summe der Primzahlen geteilt durch $\varphi(n)$, der Anzahl der möglichen Restklassen, sein. Das heißt also, $\pi_{n,a}(x)$, die Anzahl der Primzahlen kleiner oder gleich $x$, die kongruent $a$ modulo $n$ sind, sollte ungefähr $\frac{x}{\varphi(n) \ln x}$ sein. Der erste, der das beweisen konnte, war de la Vallée Poussin im Jahre 1896. Wir formulieren hier eine moderne Version dieses Resultates mit der besten zur Zeit bekannten Fehlerabschätzung

**Satz 4.2.3 (Primzahlsatz für arithmetische Progressionen)** *Sei* $\lambda(x) := (\ln x)^{3/5}(\ln\ln x)^{-1/5}$. *Für jedes* $n$ *gibt es ein positives* $c$, *sodass für* $(a,n)=1$ *gilt*

$$\pi_{n,a}(x) = \frac{1}{\varphi(n)}\,\mathrm{li}(x) + O(xe^{-c\lambda(x)}) \sim \frac{x}{\varphi(n)\ln x}. \tag{4.7}$$

Ganz in Analogie zur Riemann'schen Vermutung, die man ja auch als

$$\pi(x) = \mathrm{li}(x) + O(x^{1/2+\varepsilon}) \qquad \forall \varepsilon > 0 \tag{4.8}$$

schreiben kann, können wir auch bezüglich der Funktion $\pi_{n,a}(x)$ die folgende Aussage formulieren:

**Vermutung 4.2.4 (Erweiterte Riemann'sche Vermutung)** *Seien* $n$ *und* $a$ *zwei relativ prime natürliche Zahlen, dann gilt für jedes* $\varepsilon > 0$

$$\pi_{n,a}(x) = \frac{\mathrm{li}(x)}{\varphi(n)} + O(x^{1/2+\varepsilon}). \tag{4.9}$$

Auch zum Resultat (3.36) von Koch existiert ein Analogon, und zwar wurde etwa 30 Jahre nach Koch von E. Titchmarsh folgender Satz bewiesen:

**Satz 4.2.5 (Titchmarsh)** *Unter Annahme der Erweiterten Riemann'schen Vermutung gilt für* $(a,n) = 1, a, n \in \mathbb{N}^\times$*:*

$$\pi_{n,a}(x) = \frac{\mathrm{li}(x)}{\varphi(n)} + O(x^{1/2}(\ln x + \ln n)). \tag{4.10}$$

Man weiß also dank Dirichlet und seinem Satz 4.2.2, dass es in jeder arithmetischen Folge $kn + a$ mit $(a,n) = 1$ unendlich viele Primzahlen gibt, und man vermutet auch, dass die Primzahlen insgesamt gleichmäßig auf die $\varphi(n)$ Restklassen mod $n$ verteilt sind.

### 4.2.1 Konkrete Beispiele des Satzes

Wie bereits angekündigt, wenden wir uns nunmehr 2 konkreten Beispielen von arithmetischen Folgen zu, und werden beweisen, dass sie jeweils unendlich viele Primzahlen beinhalten; wir werden zeigen, dass die beiden Restklassen mod 4, die der Zusatzbedingung des Dirichlet'schen Primzahlsatzes 4.2.2: $(a,4) = 1$ genügen, unendlich viele Primzahlen enthalten.

Wenden wir uns zunächst dem einfacheren Fall zu. Beginnend mit der Folge $4k + 3$ zeigen wir den dem Satz 4.2.2 entsprechenden

**Satz 4.2.6** *Es gibt unendlich viele Primzahlen der Form* $4k+3$ $(k = 0, 1, \dots)$, *d.h. in der Menge der Zahlen* $\{3, 7, 11, 15, 19, \dots\}$ *gibt es unendlich viele Primzahlen.*

*Beweis:* Angenommen es gibt nur endlich viele Primzahlen dieser Gestalt, und bezeichnen wir sie mit $p_1, \dots, p_s$. Dann bilde man $N := p_1^2 \cdots p_s^2 + 2$; nach Voraussetzung gilt $p_i = 4k_i + 3$ für ein gewisses $k_i \in \mathbb{N}$ $(i = 1, \dots, s)$, also

$$p_i^2 = (4k_i + 3)^2 = 16k_i^2 + 24k_i + 9 = 4k + 1 \tag{4.11}$$

für ein $k$. Daher $(4k+3)(4l+3) = 4m+1$ für ein $m \in \mathbb{N}$. Somit hat $N = p_1^2 \cdots p_s^2 + 2$ die Form $(4n+1) + 2 = 4n + 3$.
Sei $N = q_1 \cdots q_r$ die Primfaktorzerlegung von $N \in \mathbb{N}$ $(N > 1)$. Nicht alle $q_i$ sind von der Form $4k+1$ (da sonst auch $N$ von dieser Form ist). Daher gibt es ein $q_j$, $1 \leq j \leq r$, von der Form $q_j = 4k + 3$ (Division mit Rest liefert: $0 \leq a < 4$, also $q_j = 4 \cdot k + a$. Aber $4k + 0$ und $4k + 2$ sind keine Primzahlen. $4k + 1$ ist schon ausgenommen. 2 tritt nicht als Faktor auf, da $N = 4k + 3$ ungerade ist).
Es folgt: $q_j = p_i$ für ein $i$ $(1 \leq i \leq s)$ wobei $q_j \mid N$ und $q_j = p_i \mid p_1^2 \cdots p_s^2 \Rightarrow q_j \mid N - p_1^2 \cdots p_i^2 \cdots p_s^2 = 2$, also $q_j \leq 2$ - Widerspruch $(q_j = 4k + 3 \geq 3)$ □

Das zweite Beispiel, die arithmetische Folge $4k + 1$, ist etwas schwieriger zu untersuchen. Wir benötigen in dem nun folgenden Beweis einen nicht ganz trivialen Satz über das Legendre-Symbol, nämlich den Ersten Ergänzungssatz zum quadratischen Reziprozitätsgesetz (siehe Satz 1.1.8). Damit folgt jedoch der Beweis des entsprechenden Satzes unmittelbar:

**Satz 4.2.7** *Es gibt unendlich viele Primzahlen der Form* $4k + 1$ $(k \in \mathbb{N}^\times)$.

*Beweis:* Angenommen es gibt nur endlich viele dieser Form und bezeichnen wir sie mit $p_1, \dots, p_n$. Sei $N := (2p_1 \cdots p_n)^2 + 1$, dann gilt: $N = 2m + 1$, also ungerade, d.h. $2 \nmid N$.
Wegen $N > 1$ gibt es eine Primzahl $p$ mit $p \mid N$; d.h. $N \equiv 0(p)$. Also: $(2p_1 \cdots p_n)^2 \equiv -1(p)$. D.h. $-1$ ist quadratischer Rest mod $p$. Nach der Definition des Legendre-Symbols entspricht dies also $\left(\frac{-1}{p}\right) = 1$. Nach dem Ersten Ergänzungssatz 1.1.8 folgt nun unmittelbar

$$1 = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \Leftrightarrow \frac{p-1}{2} = 2k \ (k \in \mathbb{N}^\times) \Leftrightarrow p - 1 = 4k, \tag{4.12}$$

also $p = 4k + 1$. Nach unserer Annahme folgt: $p = p_i$ für ein $1 \leq i \leq n$. Daher gilt $p \mid (2p_1 \cdots p_n)^2$; wegen $p \mid N$ folgt: $p \mid N - (2p_1 \cdots p_n)^2 = 1$, also $p \leq 1$ - Widerspruch! □

Über diese beiden Beispiele hinaus gibt es noch zahlreiche weitere Spezialfälle von 4.2.2, die man mitunter mit sehr ähnlichen Argumentationen beweisen kann. Wir begnügen uns damit und werfen noch einen ganz kurzen Blick auf eine etwas skurrile Variante eines uns schon sehr gut bekannten Satzes.

### 4.2.2 Das Bertrand'sche Postulat für arithmetische Progressionen

Unter dem (herkömmlichen) Bertrand'schen Postulat versteht man den Satz, dass im Intervall $(n, 2n]$ mindestens eine Primzahl existiert (siehe 2.3.1). Wir haben diese Aussage in Kapitel 2.3.1 nach [AZ01] bewiesen, wo wiederum der Beweis aus der ersten Publikation von Paul Erdös entnommen wurde. Auch in dem diesem Abschnitt zugrunde liegenden Artikel von Moree [Mor93] wird auf die Arbeit dieses außergewöhnlichen Mathematikers aufgebaut.

Wie schon so oft, kann auf einen Beweis nicht näher eingegangen werden. Um den Satz formulieren zu können, müssen zunächst noch einige Begriffe definiert werden.

**Definition 4.2.8** *Sei $d$ eine natürliche Zahl $\geq 2$, und seien $p_1, p_2, \ldots, p_h$ die Primzahlen kleiner als $d$, die $d$ nicht teilen. Dann definiert man*

$$\sigma(d) := \sum_{i=1}^{h} \frac{1}{p_i}. \tag{4.13}$$

*Davon unabhängig sei weiters*

$$\alpha(d) := d \prod_{p|d} p^{\frac{1}{p-1}}. \tag{4.14}$$

Erdös hat nun gezeigt, dass

**Satz 4.2.9 (Erdös)** *Sei $\sigma(d) < 1$ und $z > \frac{d}{(d-1)(1-\sigma(d))}$, dann liegt in jeder primitiven Restklasse mod $d$ wenigstens eine Primzahl im Intervall $(x, zx]$ für jedes hinreichend große $x$.*

In [Mor93] findet sich weiters der etwas technisch anmutende Satz:

**Satz 4.2.10** *Sei $\sigma(d) < 1$ und $z > \frac{d}{(d-1)(1-\sigma(d))} (= z_{min})$, dann gibt es für jedes $m \geq 1$ eine reelle Zahl $y_m$, mit*

1. $y_m \geq d$

2. $y_m \left(z - 1 - \sigma(d)z - \frac{1}{d-1}\right) \ln \alpha(d) > 2.152\sqrt{d(zy_m + 1)} + (\pi(d) + 1 + m) \ln(d(zy_m + 1))$.

*Darüber hinaus gilt für jedes $x \geq x_m := (y_m + 1)d$, dass das Intervall $(x, zx)$ mindestens $m$ Primzahlen für jede primitive Kongruenzklasse mod $d$ enthält.*

Es wird also bewiesen, dass jedes Intervall der Form $(x, zx)$ mindestens $m$ Primzahlen $\equiv a(d)$ enthält, solange $z, a$ und $d$ gewisse Eigenschaften erfüllen.

## 4.3 Arithmetische Primzahlfolgen

Zum Abschluss des Kapitels sollen noch arithmetische Folgen untersucht werden, die nur aus aufeinanderfolgenden Primzahlen bestehen. Sie werden in dieser Arbeit der Einfachheit halber „arithmetische Primzahlfolgen“ genannt.

Es handelt sich dabei um Folgen der Form $kd + p, k = 0, 1, \ldots$, wobei jedes Element dieser Folge eine Primzahl ist, und die dazwischen liegenden Zahlen alle zusammengesetzt sind. Ein Beispiel für eine solche arithmetische Primzahlfolge ist etwa $p = 121.174.811$ und $d = 30, k = 0, 1, 2, 3, 4$.

A. Schinzel und W. Sierpiński äußerten die Vermutung, dass es beliebig viele aufeinanderfolgende Primzahlen in arithmetischen Progressionen gibt, dass es also zu jedem $n \in \mathbb{N}^\times$ eine Folge von Primzahlen $p_1, p_2, \ldots, p_n$ gibt, mit $p_i - p_{i-1} = d$, und für alle $p_{i-1} < q < p_i$ gilt $q \notin \mathbb{P}$. Eine groß angelegte Suche mittels Computer war die Folge dieser Vermutung, und für einige $n$ hat man auch bereits Beispiele gefunden, wenngleich man wie so oft von einem allgemeinen Beweis der Vermutung weit entfernt ist.

Grosswald stellte eine schärfere Vermutung in Anlehnung an Hardy und Littlewood bezüglich einer asymptotischen Schätzung der Anzahl der arithmetischen Primzahlfolgen der Länge $m$ auf, wo jeder Term $\leq x$ ist (siehe [Gro82]). Außer in dem Fall, dass $m$ der erste Term der Folge ist, muss eine arithmetische Primzahlfolge der Länge $m$ eine konstante Differenz zwischen ihren Folgegliedern besitzen, die ein Vielfaches von $\prod(m)$, dem Produkt aller Primzahlen $p \leq m$, ist.

Pritchard wiederum verallgemeinerte die Formel von Grosswald auf arithmetische Primzahlfolgen der Länge $m$ mit einer Differenz, die durch $\prod(n)$ geteilt wird $(m \leq n)$. Somit wird im Folgenden die gemeinsame Differenz $d$ in der arithmetischen Primzahlfolge als $f \cdot \prod(n)$, mit $n \in \mathbb{P}$ und maximal, dargestellt.

In Tabelle 4.2 sind einige Beispiele von arithmetischen Primzahlfolgen aufgelistet, die wenigstens aus 20 Gliedern bestehen.

| $L$ | $p$ | $f$ | $n$ | $L$ | $p$ | $f$ | $n$ |
|---|---|---|---|---|---|---|---|
| 20 | 68.469.367.129 | 4.926 | 19 | 20 | 3.313.355.036.261 | 10.878 | 19 |
| 20 | 109.405.841.773 | 29.684 | 19 | 20 | 3.362.427.181.159 | 5.956 | 19 |
| 20 | 214.861.583.621 | 1.943 | 19 | 20 | 3.774.669.829.057 | 3.205 | 19 |
| 20 | 474.054.896.773 | 6.321 | 19 | 20 | 4.251.333.799.021 | 7.833 | 19 |
| 20 | 803.467.381.001 | 9 | 23 | 20 | 4.252.782.701.327 | 2.470 | 19 |
| 20 | 882.050.255.881 | 10.525 | 19 | 21 | 2.930.617.401.661 | 29.465 | 19 |
| 20 | 1.140.997.291.211 | 788 | 19 | 21 | 5.749.146.449.311 | 2.681 | 19 |
| 20 | 1.361.328.929.537 | 19.511 | 19 | 21 | 14.676.404.481.107 | 345 | 29 |
| 20 | 2.364.458.499.701 | 11.583 | 19 | 21 | 11.410.337.850.553 | 20.660 | 23 |
| 20 | 2.750.642.120.531 | 4.663 | 19 | 21 | 28.383.220.937.263 | 8.343 | 23 |
| 20 | 2.773.814.832.407 | 155 | 19 | | | | |

Tabelle 4.2: Einige arithmetische Primzahlfolgen der Form $p + f\prod(n)$ der Länge $L \geq 20$.

Wie bei den Primzahlen, gibt es auch bei der Länge der Primzahlfolgen mit konstantem Abstand ein „Größenwettrennen“. Derzeit liegt der Rekord bei $n = 22$ (vgl. [PMT95]) aus dem Jahr 1993 mit

$$11.410.337.850.553 + 4.609.098.694.200k \qquad k = 0, 1, \ldots, 21. \tag{4.15}$$

Für weitere Informationen siehe [LP67], [DN97], bzw. [Guy98].

# Kapitel 5

# Primzahlkonstellationen

Wir haben in den bisherigen Kapiteln schon des öfteren festgestellt, wie wenig Ergebnisse auf dem Gebiet der Primzahlverteilung im Allgemeinen und der Anzahlsätze im Speziellen als gesichert, also bewiesen, anzusehen sind. Am Beispiel des Primzahlsatzes 3.2.1 etwa zeigt sich weiters, dass die wenigen Beweise oft sehr umfangreich und kompliziert sind, sodass sie in kurzer Form meist nicht vernünftig beschrieben werden können.

Am Ende dieser Arbeit soll auf ein ebenso faszinierendes wie spekulatives Gebiet der Primzahltheorie eingegangen werden. Auch wenn der Begriff der Vermutung schon in den vorangegangenen Kapiteln allgegenwärtig ist, fällt doch auf, dass bezüglich der Primzahlkonstellationen die Beweise noch dünner gesät sind.

## 5.1 Einführung

Der eingangs bereits erwähnte Primzahlsatz 3.2.1 sagt aus, dass die mittlere Dichte von Primzahlen im Bereich von $x$ etwa $\frac{1}{\ln x}$ beträgt. Das bedeutet, falls wir in einem Intervall der Länge $\Delta x$ rund um $x$ ($\Delta x$ klein bezüglich $x$) eine Zahl $t$ wählen, dann wird die Wahrscheinlichkeit, dass $t$ prim ist, gegen $\frac{1}{\ln x}$ streben für $x \to \infty$. Dieser Umstand deutet darauf hin, dass die Primzahlen immer seltener werden, je größer $x$ wird - eine Beobachtung, die bereits zu Beginn unserer Untersuchungen im Zusammenhang mit dem Satz von Euklid 2.1.2 gemacht wurde.

Dies bedeutet jedoch auch, dass die Abstände zwischen aufeinanderfolgenden Primzahlen $p_{n+1} - p_n$ im Mittel immer größer werden. Wie passt es jedoch dazu, dass man, soweit Primzahltabellen existieren, immer wieder auf

aufeinanderfolgende Primzahlen stößt, für die $p_{n+1} - p_n = 2$ gilt? Man nennt solche Paare von Primzahlen $p, p+2$ auch „Primzahlzwillinge“, womit wir ein erstes Beispiel für eine Primzahlkonstellation kennen. (Eigentlich ist das nicht ganz richtig, denn es wurden bereits in Abschnitt 4.3 über arithmetische Primzahlfolgen Konstellationen der Form $p, p+d, \ldots, p+kd$ vorgestellt.)

Wie schon so oft, stellen wir uns auch hier gleich die Frage, ob das ständige Finden eines weiteren Beispiels für Primzahlzwillinge etwa darin begründet ist, dass es unendlich viele gibt. Und wie sieht es etwa mit einer Formel aus, die es ermöglicht, die Anzahl der Primzahlzwillinge unter einer gegebenen Größe asymptotisch zu bestimmen?

Wir wollen uns dieser Frage zunächst wieder heuristisch nähern. Der junge Gauss hat seinerzeit vermutet, dass die Wahrscheinlichkeit dafür, dass eine beliebige Zahl in der Nähe von $x$ prim ist, etwa $1/\ln x$ ist. Somit gelangte er zu der Vermutung, dass

$$\pi(x) \approx \int_2^x \frac{dt}{\ln t}. \tag{5.1}$$

Was wäre, wenn wir 2 Primzahlen in der Umgebung von $x$ wählen? Betrachtet man deren Primalität zunächst wieder als voneinander unabhängige Ereignisse, sollte die Wahrscheinlichkeit dafür, dass beide Zahlen prim sind, etwa $1/\ln^2 x$ betragen. Führt man die Funktion $\pi_2(x)$ wie folgt

$$\pi_2(x) := |\{p \leq x | p, p+2 \in \mathbb{P}\}| \tag{5.2}$$

ein, dann gelangt man zu der Vermutung

$$\pi_2(x) \sim \int_2^x \frac{1}{\ln^2 t}\, dt. \tag{5.3}$$

Es wurde bei diesen Überlegungen jedoch mit der Annahme, die Primalität der einzelnen Zahlen sei voneinander unabhängig, ein Fehler begangen. Unter der Voraussetzung, dass $p$ ungerade ist, hat $p+2$ die doppelte Wahrscheinlichkeit, dass $2 \nmid p+2$ gilt, im Vergleich zu einer willkürlichen Wahl von $p+2$. Zufällige ungerade Zahlen haben somit die doppelte Wahrscheinlichkeit prim zu sein, wie beliebige Zahlen, die nicht von vornherein ungerade sein müssen.

Es wird daher notwendig werden, noch verschiedene Korrekturterme in Betracht zu ziehen, sodass man auf eine Schätzung der Form

$$\pi_2(x) \sim C \int_2^x \frac{1}{\ln^2 t}\, dt \tag{5.4}$$

gelangt, wobei $C$ zunächst eine beliebige reelle Zahl sein soll. Im Folgenden werden diese Konstanten noch genauer untersucht. Vorher führen wir jedoch einen wichtigen Begriff in der Analyse der Konstellationen von Primzahlen ein.

### 5.1.1 Zulässige Konstellationen

Es scheint nicht sinnvoll zu sein, jede beliebige Konstellation von Zahlen zu untersuchen. So kann sich etwa für die Konstellation $[t, t+1]$ nur die eine Lösung $t = 2$ finden, was eine weitere Untersuchung überflüssig macht. Ebenso existiert für die Konstellation $[t, t+2, t+4]$ nur eine einzige Lösung. Wie aber kann man „sinnvolle" Konstellationen erkennen? Dazu führt man den Begriff der sogenannten „zulässigen" Konstellation ein, und versteht darunter

**Definition 5.1.1 (Zulässige Konstellation)** *Eine beliebige Konstellation von natürlichen Zahlen der Bauart*

$$t + a_1, t + a_2, \ldots, t + a_l \tag{5.5}$$

*wird als zulässig bezeichnet, wenn durch keine Teilbarkeitsbeziehungen verhindert wird, dass sie zur Gänze aus Primzahlen bestehen kann.*

Diese etwas theoretische Definition soll anhand eines Beispiels näher erläutert werden. Die oben betrachtete Konstellation $[t, t+2, t+4]$ ist in der „neuen" Schreibweise gleich $[t+1, t+3, t+5]$, und ist nicht zulässig, weil je drei aufeinanderfolgende gerade oder ungerade Zahlen genau ein Vielfaches von 3 enthalten. Daran ändert auch nichts, dass die drei Primzahlen $3, 5, 7$ durchaus ein Beispiel einer obigen Konstellation bilden. Es sind nur Konstellationen interessant, bei denen es mehrere verschiedene Beispiele gibt. Dies ist hier nicht der Fall.

Um festzustellen, ob eine gegebene Konstellation zulässig ist oder nicht, gibt es eine im Prinzip einfache, wenngleich in der Praxis oft sehr arbeitsintensive (für großes $l$), Strategie. Man versucht das Intervall von $[a_1, a_l]$ mit den Primzahlen $2, 3, 5, \ldots$ so zu sieben, dass die Zahlen $a_i$ der zu untersuchenden Konstellation nicht getroffen werden. Wenn das für alle Primzahlen $p \leq l$ gelingt, dann handelt es sich um eine zulässige Konstellation im Sinne der obigen Definition, ansonsten ist sie nicht zulässig.

Die Vorgehensweise erinnert ein bisschen an das klassische Sieb des Erathosthenes, jedoch sind in diesem Fall alle Startwerte für das erste Vielfache

der Primzahlen zugelassen. Untersuchen wir beispielsweise die Konstellation

$$t+1, t+7, t+11, t+13, t+17, t+19, t+23, t+29. \tag{5.6}$$

Da sämtliche $a_i$ die gleiche Parität aufweisen, brauchen wir die Primzahl 2 nicht zu betrachten, solange wir nur das $t$ gerade wählen. Es gibt drei verschiedene Wege, das Intervall $[1, 29]$ mit der Primzahl 3 zu sieben:

$$1, 4, 7, 10, 13, 16, 19, 22, 25, 28$$
$$2, 5, 8, 11, 14, 17, 20, 23, 26, 29$$
$$3, 6, 9, 12, 15, 18, 21, 24, 27.$$

In der letzten Zeile taucht kein $a_i$ für $1 \leq i \leq 8$ auf. Das bedeutet also, dass, wenn wir $t \equiv 0(3)$ wählen, soweit noch alles in Ordnung ist. Auch für die Primzahl $p = 5$ bleibt genau eine Möglichkeit über, in der kein $a_i$ vorkommt:

$$5, 10, 15, 20, 25.$$

Bisher wissen wir also, dass wir $t \equiv 0(30)$ wählen müssen, um mit keiner der ersten 3 Primzahlen zu kollidieren. Für die Primzahl 7 ergeben sich folgende sieben Siebe:

$$1, 8, 15, 22, 29 \qquad 2, 9, 16, 23 \qquad 3, 10, 17, 24 \qquad 4, 11, 18, 25$$
$$5, 12, 19, 26 \qquad 6, 13, 20, 27 \qquad 7, 14, 21, 28$$

Jede dieser sieben Möglichkeiten enthält zumindest ein $a_i$, sodass die Konstellation (5.6) als unmittelbare Folgerung dieser Tatsache nicht zulässig ist.

Dieser Umstand kann auch algebraisch so ausgedrückt werden, dass die $a_i$ der Konstellation sämtliche sieben Restklassen modulo 7 repräsentieren:

$$7 \equiv 0, 1 \equiv 1, 23 \equiv 2, 17 \equiv 3, 11 \equiv 4, 19 \equiv 5, 13 \equiv 6(7). \tag{5.7}$$

Somit liegt praktisch bereits eine einfachere Beschreibung der Vorgangsweise auf der Hand, um über die Zulässigkeit einer Konstellation zu entscheiden. Alles was zu tun ist, ist zunächst einen (beliebigen) Wert für $t$ zu fixieren, und danach sämtliche $t + a_i \bmod p$ für alle $a_i$ der Konstellation zu berechnen. Bleibt dabei zumindest eine Restklasse mod $p$ frei, und zwar für jedes $p \leq l$, dann und nur dann ist die Konstellation zulässig. Der Grund, warum nur Primzahlen $\leq l$, also der Länge der Konstellation, betrachtet werden müssen, ist klar: es ist unmöglich, mit $l$ Elementen mehr als $l$ verschiedene Restklassen zu besetzen.

Somit wollen wir nochmals für (5.6) die Untersuchung nach dem neuen Algorithmus durchführen und gelangen zum Ergebnis:

| | | |
|---|---|---|
| Belegte Restklassen | mod 2 | 1 |
| | mod 3 | 1, 2 |
| | mod 5 | 1, 2, 3, 4 |
| | mod 7 | 0, 1, 2, 3, 4, 5, 6 |

Da alle sieben Restklassen mod 7 belegt sind, folgt wiederum, dass die Konstellation nicht zulässig ist.

Nunmehr wenden wir uns wieder den Konstanten „C“ aus (5.4) zu.

### 5.1.2 Die Hardy-Littlewood'schen Konstanten

Bis jetzt können wir also bei einer gegebenen Konstellation entscheiden, ob sich eine nähere Betrachtung lohnt, oder ob es aus bestimmten Gründen unmöglich ist, dass jedes Element davon eine Primzahl ist.

Wir wollen noch kurz bei den eben betrachteten Restklassen bleiben. Offensichtlich repräsentiert jede freigebliebene Restklasse mod $p$ eine Möglichkeit, mit Vielfachen von $p$ zu sieben. Betrachtet man beispielsweise die Quadrupel $(t, t+2, t+6, t+8)$, so stellt sich heraus, dass für die Primzahlen 2 und 3 jeweils nur eine Restklasse ($\equiv 1(2), \equiv 2(3)$) frei bleibt. Dies reduziert insgesamt die Möglichkeiten für $t$ auf eine von 6 Restklassen. Wählt man aber $t \equiv 5(6)$, dann erhöht das die Wahrscheinlichkeit, dass alle 4 Zahlen $\in \mathbb{P}$ sind, um den Faktor $\left(\frac{2}{1} \cdot \frac{3}{2}\right)^4 = 81$ (im Vergleich zur zufälligen Wahl aller 4 Zahlen). Somit liefert dies insgesamt einen Faktor von $\frac{81}{6}$.

Wie aber kommt man auf solche Werte? Nun, die Wahrscheinlichkeit, dass eine beliebige natürliche Zahl $n \in \mathbb{N}$ prim ist, wurde ganz zu Beginn von Kapitel 2 mit

$$\mathcal{W}(n \in \mathbb{P}) = \prod_{p \in \mathbb{P}, p \leq \sqrt{n}} \left(1 - \frac{1}{p}\right) \tag{5.8}$$

angegeben. Jede Primzahl steuert also einen Faktor $\frac{p-1}{p}$ zum Produkt bei. Wählt man die Zahl $n$ willkürlich, dann muss das gesamte Produkt betrachtet werden. Wird jedoch jene Restklasse ausgewählt, die von den 6 Möglichkeiten mod 2 und 3 übrigbleibt, so kann die Zahl $n$ nicht durch zwei oder drei geteilt werden. Die Wahrscheinlichkeit (5.8) ist also gewissermaßen durch

$$\mathcal{W}'(n \in \mathbb{P}) = \prod_{p \in \mathbb{P}, 5 \leq p \leq \sqrt{n}} \left(1 - \frac{1}{p}\right) = \frac{2}{1}\frac{3}{2} \prod_{p \in \mathbb{P}, p \leq \sqrt{n}} \left(1 - \frac{1}{p}\right) \tag{5.9}$$

zu ersetzen. Das erklärt auch die beiden obigen Faktoren. Allgemein muss also der Beitrag $\frac{p-1}{p}$ jener Primzahl $p$, von der feststeht, dass sie als Teiler nicht in Frage kommt, mit $\frac{p}{p-1}$ sozusagen „neutralisiert“ werden. Wenn man dann noch bedenkt, dass diese Betrachtungen für jede einzelne Zahl gelten, gelangt man schließlich zu dem gewünschten Wert von 81.

Bleibt die Frage zu klären, warum man bei 3 aufhören kann, die Anzahl der freien Restklassen zu bestimmen, bzw. den Wert der ursprünglichen Wahrscheinlichkeit zu korrigieren. Auch dies soll allgemein überlegt werden.

Es ist klar, dass man für die Primzahl $p > a_l$, wobei $a_l$ wie üblich das größte Element in der zu untersuchenden Konstellation darstellt, mit genau $p - l$ freien Restklassen rechnen kann, sodass eine Untersuchung der ersten $\pi(a_l)$ Primzahlen ausreichend ist. Eigentlich kann man sich sogar auf jene Primzahlen beschränken, für die $p \leq a_l - a_1$ gilt, wie folgende Überlegungen zeigen:

Für die Primzahl $p > l$ bleiben mindestens $p - l$ Restklassen frei, da es für $p > l$ mehr als $l$ Restklassen gibt. Somit können höchstens $l$ verschiedene Restklassen belegt werden. Es wäre jedoch möglich, dass zwei verschiedene Elemente $a_i$ und $a_j$ in einer Restklasse landen, dass also mehr als $p - l$ Restklassen frei bleiben. Das würde bedeuten

$$a_i \equiv a_j(p) \Rightarrow p \mid a_i - a_j \Rightarrow p \leq a_i - a_j. \tag{5.10}$$

Daraus ist ersichtlich, dass die Primzahlen bis zum Maximum der Differenzen der $a_i$ gesondert untersucht werden müssen. Benötigt man die ersten $l$ Primzahlen zur Bestimmung der Zulässigkeit einer Konstellation, so muss man bei der Bestimmung der Konstanten $C$ die Primzahlen

$$p \leq \max_{i=1,\ldots,l} a_i - \min_{j=1,\ldots,l} a_j \tag{5.11}$$

in Betracht ziehen. Auch wenn nicht explizit gefordert, so ist es doch aus Gründen der Eindeutigkeit der Darstellung von Konstellationen sinnvoll, $a_i < a_j$ für $i < j$ zu verlangen, sodass sich (5.11) schließlich als $p \leq a_l - a_1$ schreiben lässt. (5.11) wird später in den Implementierungen in DERIVE verwendet, um unnötigen Rechnungen aus dem Weg zu gehen.

Es ist also klar, dass für jede Primzahl $p > 8 - 0 = 8$ je $p - 4$ Möglichkeiten existieren, $t$ zu wählen, ohne dass $t, t+2, t+6, t+8$ Vielfache von $p$ sind. Dem gegenüber stehen je $p-1$ Möglichkeiten, wenn die $t$'s unabhängig voneinander

gewählt werden. Für diese $p$ ergibt sich somit ein Faktor von

$$\left(1-\frac{4}{p}\right)\left(1-\frac{1}{p}\right)^{-4}=\frac{p^3(p-4)}{(p-1)^4}. \tag{5.12}$$

Es stellt sich jedoch heraus, dass für $p=5$ und $p=7$ bereits $p-4$ Restklassen übrigbleiben, sodass die oben angeführten Korrekturen für $p=2$ und $p=3$ ausreichen. So gelangt man zu der Formel, die aus einer Vermutung von Hardy und Littlewood (siehe [HL22]) hervorgeht, und z.B. für den Fall von $(t,t+2,t+6,t+8)$ folgendermaßen aussieht:

$$\begin{aligned} P_x(p,p+2,p+6,p+8) &\backsim \frac{27}{2}\prod_{p\geq 5}\frac{p^3(p-4)}{(p-1)^4}\int_2^x\frac{dx}{\ln^4 x}\approx \\ &\approx 4.151180864\int_2^x\frac{dx}{\ln^4 x}. \end{aligned} \tag{5.13}$$

Dabei sei noch angemerkt, dass die Produkte über die involvierten Primzahlen zu nehmen sind. Das Symbol „$\backsim$“ soll andeuten, dass es sich dabei nur um vermutete Beziehungen handelt, jedoch nichts bewiesen werden konnte. $P_x(\ldots)$ bezeichnet die Anzahl der Konstellationen, deren kleinstes Mitglied $\leq x$ ist. Diese Näherungen sind natürlich für $x\to\infty$ zu betrachten.

Das Endresultat unserer Untersuchungen der Restklassen sind also jetzt Konstanten wie eben z.B. 4.151180864, die sogenannten „Hardy-Littlewood'schen Konstanten“.

Um sich mit diesem Begriff noch etwas auseinanderzusetzen, soll zum Abschluss folgende Konstellation betrachtet werden:

$$\begin{gathered} t+11,t+13,t+17,t+19,t+23,t+29,t+31, \\ t+37,t+41,t+43,t+47,t+53,t+57,t+61,t+67. \end{gathered} \tag{5.14}$$

Wir überlegen uns zunächst, dass dies eine zulässige Konstellation im Sinne der obigen Definition ist, und suchen die Darstellung nach Hardy und Littlewood. Da für $t=0$ alle Elemente $\in\mathbb{P}$ sind, sind die ersten Primzahlen $2,3,5,7$ offensichtlich nicht relevant. Die Konstellation besteht aus 15 Elementen, sodass für alle hinreichend großen Primzahlen $p$ zumindest $p-15$ Restklassen frei bleiben.

Die Primzahlen ab 11 muss man gesondert untersuchen, und es stellt sich heraus, dass im Fall $p=11$ die Restklasse $\equiv 5(11)$ frei bleibt (nach wie vor gilt $t=0$), sowie die Restklasse $\equiv 12(13)$. Für $p=17$ bleiben insgesamt 4

Restklassen über, für $p = 19$ sind es 6 und für $p = 23$ gibt es 9. Schließlich: für alle $p \geq 29$ bleiben $p - 15$ Restklassen frei.

Um jetzt die Konstanten zu berechnen, müssen die eben erhaltenen Informationen über die Restklassen verwendet werden. Somit gelangt man zu folgender Formel für die Anzahl der Konstellationen vom Typ (5.14):

$$\begin{aligned} & P_x(t+11, t+13, t+17, \ldots, t+61, t+67) \; \mathcal{L} \\ \mathcal{L} \quad & \frac{2^{14}}{1^{15}} \cdot \frac{3^{14}}{2^{15}} \cdot \frac{5^{14}}{4^{15}} \cdot \frac{7^{14}}{6^{15}} \cdot \frac{11^{14}}{10^{15}} \cdot \frac{13^{14}}{12^{15}} \cdot \frac{4 \cdot 17^{14}}{16^{15}} \cdot \frac{6 \cdot 19^{14}}{18^{15}} \cdot \frac{9 \cdot 23^{14}}{22^{15}} \cdot \\ & \prod_{p \geq 29} \frac{p^{14}(p-15)}{(p-1)^{15}} \int_2^x \frac{dx}{\ln^{15} x} \approx \\ \approx \quad & 187823.7 \int_2^x \frac{dx}{\ln^{15} x} \sim 187823.7 \cdot \frac{x}{\ln^{15} x}. \end{aligned} \tag{5.15}$$

Zu dieser Formel sei noch gesagt, dass trotz der Tatsache, dass man die Primzahlen nicht alle explizit kennt, die Konstanten dennoch in jeder beliebigen Genauigkeit berechnet werden können! Dies hängt damit zusammen, dass (3.2) so umgeformt werden kann, dass jede dieser Konstanten als konvergente Reihe bekannter Funktionen darstellbar ist.

### 5.1.3 Zwei sich widersprechende Vermutungen

Formeln wie (5.13) und (5.15) sind allesamt Spezialfälle der folgenden, großen Vermutung:

**Vermutung 5.1.2 (Prime k-Tupel Vermutung)** *Jede zulässige Konstellation tritt unendlich oft als reine Primzahlkonstellation auf, und asymptotisch ist die Anzahl der Konstellationen $\leq x$ gegeben durch*

$$\Omega\left(\frac{x}{\ln^k x}\right), \tag{5.16}$$

*wobei $k$ gleich der Länge der Konstellation ist.*

Diese Aussage ist, wie der Name schon andeutet, noch unbewiesen. Selbst der einfachste Fall, jener der Primzahlzwillinge, ist ungelöst! Aber sämtliche numerische Untersuchungen stützen 5.1.2 bis zum heutigen Tag.

Zur zweiten Vermutung: Der Primzahlsatz besagt, dass die Primzahlen immer weniger dicht liegen, je höher man in der Zahlenfolge nach oben geht. Diese Tatsache hat Hardy und Littlewood bewogen, eine weitere Hypothese aufzustellen, die

**Vermutung 5.1.3 (2. Hardy-Littlewood-Vermutung)** *In keinem Intervall* $[x+1, x+y]$ *der Länge* $y$ *gibt es mehr Primzahlen, als im Intervall* $[1, y]$. *D.h.*

$$\pi(x+y) - \pi(x) \overset{c}{\leq} \pi(y) \qquad \forall x, y. \tag{5.17}$$

Mit anderen Worten: nirgends sind die Primzahlen so dicht, wie am Anfang der Zahlenreihe. Auf den ersten Blick scheint diese Vermutung relativ plausibel zu sein. Jedoch 1974 konnten Douglas Hensley und Ian Richards [Ric74] nachweisen, dass bestimmte zulässige Konstellationen existieren, die dichter liegen als die Primzahlen zu Beginn der Zahlenreihe. Sie konnten unter Voraussetzung von 5.1.2 zeigen, dass es ein $y$ geben muss, sodass

$$\pi(y + 20.000) - \pi(y) > \pi(20.000) \tag{5.18}$$

gilt. Das würde freilich der zweiten Vermutung komplett widersprechen, sodass nur eine der beiden Vermutungen richtig sein kann (siehe auch [Veh79]). Heute geht man allgemein davon aus, dass die erste Vermutung („Prime k-Tupel Vermutung“) richtig ist, und dass sich die zweite Hardy-Littlewood Vermutung als falsch herausstellen wird, jedoch ist ein Beweis in diese Richtung noch offen.

## 5.2 Primzahlzwillinge

### 5.2.1 Einführende Bemerkungen

Eines der bekanntesten Beispiele solcher Konstellationen und gleichzeitig das einfachste bilden sicherlich die sogenannten „Primzahlzwillinge“, denen der gesamte folgende Abschnitt gewidmet ist. Es sind dies Primzahlpaare der Form $(p, p+2)$. Nach Hardy & Littlewood existieren unendlich viele davon (siehe [HL22], Theorem X1).

In der Tat ist es nicht besonders schwierig, Zahlenbeispiele von Zwillingen anzugeben:

$$\begin{aligned}(3,5), (5,7), (11,13), \ldots, (197,199), (227,229), (239,241), \ldots,\\ (1.091, 1.093), (1.151, 1.153), (1.229, 1.231), \ldots\end{aligned} \tag{5.19}$$

Auch wenn man ad hoc wohl nur die ersten drei Vertreter nennen wird, so sind doch alle Dreiergruppen interessant. Jede Gruppe besteht aus drei aufeinanderfolgenden Primzahlzwillingen. Anhand dieses Beispiels kann man

abermals erkennen, dass die Primzahlzwillinge immer weiter auseinanderzuliegen scheinen. Dennoch soll es unendlich viele geben...

Wir wollen noch einmal auf die Funktion $\pi_2(x)$ zurückkommen, und eine Darstellung der Form (5.4) anstreben. Die Hardy-Littlewood'sche Konstante $C$ in (5.4) kann mittlerweile bestimmt werden.

Nach den Überlegungen beim Studium dieser Konstanten folgt, dass man sich bei der Bestimmung von $C$ auf die Primzahl 2 konzentrieren kann. Wegen $3 > a_2 - a_1 = 2$ bleiben ab $p = 3$ genau $p-2$ Restklassen frei. Für die Primzahl 2 entsteht ein Korrekturfaktor der Form $\frac{2}{2-1} = 2$, sodass sich unmittelbar die folgende Formel ergibt:

$$\pi_2(x) \curlyeqsucc 2 \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} \int_2^x \frac{dx}{\ln^2 x} \approx 1.320323632 \int_2^x \frac{dx}{\ln^2 x} \tag{5.20}$$

Dabei wird oft mit $c_2 := 0.6601618159$ die sog. „Primzahlzwillingskonstante" bezeichnet. Trotz aller numerischer „Verifikation" bleibt es dennoch eines der großen ungelösten mathematischen Probleme, ob die Menge der Primzahlzwillinge unendlich groß ist. Ein Resultat, das damit fast übereinstimmt, ist jenes von Chen Jing-run aus dem Jahre 1966. Er konnte zu folgendem Satz einen Beweis (!) angeben:

**Satz 5.2.1 (Jing-run)** *Es gibt unendlich viele Primzahlen $p \in \mathbb{P}$, sodass $p+2$ entweder ebenfalls prim, oder aber gleich dem Produkt von 2 (anderen) Primzahlen ist.*

Bevor wir uns mit einer interessanten Tatsache im Zusammenhang mit den Primzahlzwillingen näher auseinandersetzen, wollen wir noch einige Vertreter von Zwillingspaaren kennenlernen. Am 25. Juli 1995 beispielsweise entdeckte Tony Forbes das Paar

$$6.797.727 \cdot 2^{15.328} \pm 1. \tag{5.21}$$

In [For97] werden die dazu verwendeten Routinen erklärt. Zuvor, im November 1994, konnten Karl-Heinz Indlekofer und Antal Jarai die Primalität von

$$697.053.813 \cdot 2^{16.352} \pm 1 \tag{5.22}$$

beweisen, Zahlen mit immerhin 4.932 Stellen (siehe [IJ96]). Am 16. Februar 1999 schließlich meldeten dieselben Autoren, dass sie ein neues Paar noch größerer Primzahlzwillinge gefunden hätten:

$$242.206.083 \cdot 2^{38.880} \pm 1 \tag{5.23}$$

mit unvorstellbaren 11.713 Stellen, womit ein bestehender Rekord von Harvey Dubner (5.129 Stellen) aus dem Jahre 1995 überboten wurde (siehe [IJ99]).

Weitere Arbeiten, in denen so manches interessante Detail über Primzahlzwillinge nachgelesen werden kann, sind etwa [CP79],[PSZ90].

Im Bereich der Primzahlen ist man ständig auf der Suche nach immer größeren Exemplaren einer besonderen Bauart. So wird man auch hier wieder größere finden...

### 5.2.2 Die Brun'sche Konstante

Eine echte Ausnahme in all diesen Spekulationen stellt das folgende *bewiesene* Resultat von Brun dar. Der Satz war sicherlich nicht ganz einfach zu zeigen. Es wäre wohl kein Resultat der Primzahlentheorie, wenn nicht eine gewisse Unsicherheit damit verbunden ist. Dazu kommen wir jedoch etwas später, zunächst wollen wir uns kurz mit Siebmethoden beschäftigen.

Tatsächlich sind viele Resultate der letzten Jahre nur durch besonders geschickt gewählte Siebmethoden beweisbar. Die Theorie des Siebens ist jedoch höchst komplex, sodass hier nur ein kleiner Einblick gegeben werden kann. Jedem bekannt ist das Sieb des Eratosthenes, welches beim Auffinden der Primzahlen mitunter sehr gute Dienste leistet. Es ist ein sehr einfaches Sieb, und doch ist es in gewissem Sinne speziell im Vergleich zu einem zufälligen Aussieben (vgl. Kapitel 2.1.1).

Das Brun'sche Siebverfahren dient zur Siebung der Zahlen $n \leq x$ einer arithmetischen Folge $F$ mit dem Anfangsglied $a > 0$ und der konstanten Differenz $d$. Man streicht zunächst aus der Primzahlenfolge die Zahl 2 und die Primteiler von $d$ weg. Die verbleibenden Primzahlen, der Größe nach geordnet, werden mit $q_1, q_2, \ldots$ bezeichnet; $\pi'(y)$ sei die Anzahl der $q_i \leq y$. Jedem einzelnen $q_i$ werden zwei arithmetische Folgen $A_i$ und $B_i$ mit den Anfangsgliedern $a_i$ bzw. $b_i$ und der Differenz $q_i$ zugeordnet. Dabei gelte $0 \leq a_i < q_i, 0 \leq b_i < q_i, a_i \neq b_i$. Die $2\pi'(y)$ Folgen $A_i$ und $B_i$ bilden jetzt das Sieb, indem man jene Zahlen aus $F$ streicht, die in einer Folge $A_i$ oder $B_i$ vorkommen.

Die übrigbleibenden $n \leq x$ erfüllen also die Bedingungen

1. $n \equiv a(d)$

2. $n \not\equiv a_i(q_i)$

3. $n \not\equiv b_i(q_i), a_i \neq b_i$.

Die Anzahl dieser $n$ bezeichnen wir mit $N(d, x, y)$. Das Ziel des Siebverfahrens ist jetzt die Gewinnung von möglichst guten Abschätzungen für diese Größe.

Wir wollen uns kurz folgendem Beispiel zuwenden: Sei $a = 1, d = 2$,$q_1 = 3$, $q_2 = 5, q_i = p_{i+1}; a_i = 0 \ \forall i; b_i \equiv x(q_i)$ für $x \not\equiv 0(q_i)$ und $b_i \not\equiv x(q_i)$ für $x \equiv 0(q_i)$. Ist $x$ gerade, und $u \geq 2$ ganz, dann ist $N(2, x, x^{1/u})$ die Anzahl der ungeraden $n \leq x$ mit der Eigenschaft, dass weder $n$ noch $n - x$ durch eine Primzahl $p \leq x^{1/u}$ teilbar sind. (Aus $x - n \equiv 0(q_i)$ folgt nämlich, dass $n \equiv b_i(q_i)$ für $x \not\equiv 0(q_i)$ und $n \equiv 0(q_i)$ für $x \equiv 0(q_i)$.) Sämtliche Primteiler von $n$ und $n - x$ sind also größer als $x^{1/u}$, insbesondere haben sowohl $n$ als auch $x - n$ höchstens $u - 1$ Primfaktoren.

Damit ließe sich die *Goldbach'sche Vermutung* 2 in der harmlos anmutenden Form $N(2, x, x^{1/2}) \geq 2$ schreiben.

Mit Hilfe des Siebverfahrens nach Brun lässt sich schließlich über die Anzahl $N(d, x, x^{1/u})$ allgemein folgende Aussage herleiten

$$N(d, x, x^{1/u}) = \Omega\left(\frac{C(u)x}{\ln^2 x}\right). \tag{5.24}$$

Der Weg dahin ist mitunter beschwerlich und mühsam. Der interessierte Leser sei an dieser Stelle auf das Buch von Trost [Tro53] verwiesen, wo dieser umrissen wird.

Auf das oben angekündigte berühmte Resultat gelangt man nun folgendermaßen: Aus der Folge der ungeraden Zahlen $n$ $(a = 1, d = 2)$ sollen die Primzahlzwillinge $\leq x$ ausgesiebt werden. $n-2$ und $n \leq x$ sind beides Primzahlen $> \sqrt{x}$, wenn sie durch kein $p_i \leq \sqrt{x}$ teilbar sind, das heißt, wenn $n \not\equiv 0(p_i), n - 2 \not\equiv 0(p_i)$ gilt. Dann ergibt sich also für $\pi_2(x)$, die Anzahl der Primzahlzwillinge $\leq x$, aus (5.24)

$$\pi_2(x) = N(2, x, x^{1/2}) + \pi_2(\sqrt{x} + 2) < \frac{C_1 x}{\ln^2 x} + \sqrt{x} + 2 < \frac{Cx}{\ln^2 x}. \tag{5.25}$$

Ist $t_m$ die größere Primzahl im $m$-ten Zwillingspaar, so gilt also

$$m < \frac{Ct_m}{\ln^2 t_m} \qquad \text{oder} \qquad \frac{1}{t_m} < \frac{C}{m \ln^2 t_m} < \frac{C}{m \ln^2 m}. \tag{5.26}$$

Da $\sum \frac{1}{m \ln^2 m}$ nach (1.35) konvergiert, erhalten wir den von Brun 1919 bewiesenen

**Satz 5.2.2 (Brun)** *Sei $\mathbb{P}_2$ die Menge der Primzahlzwillinge. Dann gilt entweder $|\mathbb{P}_2| < \infty$, wenigstens aber*

$$\sum_{p \in \mathbb{P}_2} \frac{1}{p} < \infty. \tag{5.27}$$

Die Summe über die Reziprokwerte der Primzahlzwillinge konvergiert also! Das bedeutet, dass die Primzahlzwillinge wesentlich seltener sind, als die Primzahlen selbst, denn deren Summe über die Reziprokwerte divergiert bekanntlich (siehe Satz 2.1.4).

Der Grenzwert dieser Summe (5.27) wird nach ihrem Schöpfer auch „Brun'sche Konstante“ genannt, und oft mit „$B$“ bezeichnet. Nicht ganz klar ist jedoch manchmal, welche Zahl sich hinter der Brun'schen Konstante tatsächlich verbirgt, gehen doch auf verschiedene Autoren verschiedene Definitionen zurück. Wir wollen unter der Brun'schen Konstante folgende Summe verstehen:

$$B = \frac{1}{3} + \frac{1}{5} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \frac{1}{19} + \cdots . \tag{5.28}$$

Selmer berechnete

$$S = \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \cdots , \tag{5.29}$$

also ohne dem ersten Primzahlpaar $(3, 5)$. Fröberg wiederum summiert nur einmal über die Primzahl 5:

$$F = \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \cdots , \tag{5.30}$$

während bei Karst selbst die Form

$$K = 1 + \frac{1}{3} + \frac{1}{3} + \frac{1}{5} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \cdots \tag{5.31}$$

auftaucht. Es gilt, wie man sich unschwer davon überzeugen kann, allenfalls folgender Zuammenhang

$$B = S + \frac{8}{15} = F + \frac{1}{5} = K - \frac{4}{3}. \tag{5.32}$$

Wir bevorzugen die Bezeichnung $B$, gibt sie doch auch die natürliche Art und Weise Primzahlzwillinge zu zählen wieder. An dieser Stelle sei allerdings

angemerkt, dass Brun seinerzeit die Fröberg'sche Form betrachtete, da er die Primzahlpaare der Form $6 \mp 1$ studierte.

Um die Brun'sche Konstante explizit zu berechnen, bedient man sich nunmehr der bekannten Primzahlzwillinge, und korrigiert die daraus resultierende Summe der Form

$$\sum_{p \in \mathbb{P}_2, p \leq q} \frac{1}{p} \tag{5.33}$$

mit einem Faktor, der sich aus der Annahme der Richtigkeit der 5.1.2 entsprechenden Aussage für Primzahlzwillinge ergibt. Diese Rechnungen wollen wir uns im Folgenden kurz überlegen.

Ausgangspunkt ist die Richtigkeit der Vermutung von Hardy-Littlewood. Es soll also folgende Beziehung gelten:

$$\pi_2(x) \overset{\mathcal{L}}{\sim} 2c_2 \int_2^x \frac{dx}{\ln^2 x}, \tag{5.34}$$

wobei $c_2$ die Primzahlzwillingskonstante bezeichnet. Weiters kennt man sämtliche Primzahlzwillinge unterhalb einer Grenze $q$, sodass die Summe über die Reziprokwerte für Primzahlpaare kleiner oder gleich $q$ tatsächlich berechnet werden kann. Für die Anzahl der Primzahlzwillinge unterhalb von $q$ müsste etwa gelten

$$\pi_2(q) \overset{\mathcal{L}}{\sim} 2c_2 \int_2^q \frac{dx}{\ln^2 x}. \tag{5.35}$$

Somit ergibt sich für die Anzahl jener Zwillinge, die unbekannt sind, bzw. nicht in der exakten Summe berücksichtigt werden

$$2c_2 \int_q^\infty \frac{dx}{\ln^2 x}. \tag{5.36}$$

Folglich erscheint es klar, dass die mit den Primzahlzwillingen bis $q$ erhaltenen Werte für $B$ durch einen Term der Form

$$2c_2 \int_q^\infty \frac{2\,dx}{x \ln^2 x} = 4c_2 \cdot \lim_{r \to \infty} \int_q^r \frac{dx}{x \ln^2 x} = \frac{4c_2}{\ln q} \tag{5.37}$$

korrigiert werden müssen (siehe etwa [SW74], [Bre75]). Auf diese Weise gelangt man auf die jeweils aktuellen Werte der Brun'schen Konstante $B$. Derzeit ist der genaueste Wert

$$B = 1.9021605822\ldots \pm 8 \cdot 10^{-10}. \tag{5.38}$$

Um diesen Wert zu bestimmen, hat Nicely die Primzahlzwillinge bis $2.75 \cdot 10^{15}$ zur Berechnung herangezogen, und danach mit Hilfe von (5.37) extrapoliert, um den genauen Wert von $B$ zu approximieren (siehe auch [19]). Seine früheren Berechnungen brachten 1995 den nunmehr berühmten Fehler im Pentium-Chip zutage. Diese Entdeckung kostete den Verantwortlichen Millionen von Dollar (siehe auch [Nic95]).

Bewiesen im Zusammenhang mit dem Wert der Brun'schen Konstante ist lediglich, dass folgende Ungleichung gilt

**Lemma 5.2.3** *Bezeichne $B$ die Brun'sche Konstante wie in (5.28) definiert, dann gilt*

$$1.82 < B < 2.15. \tag{5.39}$$

## 5.3 Untersuchungen mittels DERIVE

In diesem Abschnitt soll das bisher Bekannte genutzt werden, um in DERIVE die Möglickeiten zu schaffen, mit Hilfe dieses Computeralgebrasystems einige Beispiele von Konstellationen untersuchen zu können.
Der erste Begriff, den wir kennenlernten, war der Begriff der zulässigen (engl. *„admissible“*) Konstellation. Wir wollen im Folgenden diese Bezeichnungen, sofern nicht anders angegeben, verwenden: unter $p$ sei wie immer eine beliebige Primzahl gemeint, und „$a$“ bezeichne einen Vektor, der die Konstellation repräsentiert. Das Primzahltripel $t, t+2, t+6$ werde beispielsweise so kodiert: $a = [0, 2, 6]$.

Beim Begriff der zulässigen Konstellation war zu überprüfen, ob modulo $p$ eine freie Restklasse in $a$ existiert. Eine einfache Möglichkeit, dies zu entscheiden, bietet

```
free(a, p, i_ := 0) :=
  Prog
    a := MOD(a, p)
    Loop
      If NOT MEMBER?(i_, a)
         RETURN true
      If i_ = p - 1
         RETURN false
      i_ :+ 1
```

Mit Hilfe von `free(a, p)` kann eine Funktion geschrieben werden, die überprüft, ob eine Konstellation der Form (5.5) zulässig ist, oder nicht. Dabei sollen die $a_i$ wieder im Vektor $a$ abgespeichert sein.

```
admissible(a, i_ := 2) :=
  Loop
    If NOT free(a, i_)
       RETURN false
    If i_ >= DIM(a)
       RETURN true
    i_ := NEXT_PRIME(i_)
```

Mit Hilfe dieser Funktion ergbit sich somit

```
admissible([0, 1]) = false
admissible([0, 2]) = true
admissible([0, 2, 4]) = false
admissible([0, 2, 6]) = true
admissible([0, 4, 6]) = true
```

Bei der kommenden Aufgabenstellung steht die Frage im Mittelpunkt, welche Restklassen explizit im Vektor $a$ mod $p$ enthalten sind. Diese kann in DERIVE durch den Einsatz von Listen gelöst werden. Während es den Vektor

```
[0, 1, 1, 2, 2, 2, 3]
```

durchaus gibt, wird die Liste mit den gleichen Elementen folgendermaßen vereinfacht:

```
{0, 1, 1, 2, 2, 2, 3} = {0, 1, 2, 3},
```

d.h. notiert werden nicht die einzelnen Elemente, sondern nur die verschiedenen, ohne deren Vielfachheit. Dies ist jedoch genau das hier Benötigte. Somit ergibt sich ohne große Schwierigkeiten

```
rest(a, p) :=
  SORT(VECTOR(j_,j_,MAP_LIST(MOD(aSUBi_,p),i_,{1,...,DIM(a)})))
```

Bei dem Beispiel von Riesel [Rie94], der die Konstellation (5.14) betrachtete, welche wir der Einfachheit halber mit

```
                    riesel :=
  [11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67]
```

abkürzen wollen, ergibt obiges Program für $p = 17$ folgenden Output:

```
                    rest(riesel, 17) =
        [0, 2, 3, 6, 7, 8, 9, 10, 11, 12, 13, 14, 16].
```

Es wäre desweiteren sehr interessant, wie man mit Hilfe der bisherigen Routinen die Hardy-Littlewood'sche Form für $P_x(a)$, der Anzahl der Konstellationen vom Typ $a$, die kleiner als $x$ sind, möglichst automatisiert erstellen kann. Die hinteren Glieder sind dabei ohnedies festgelegt, sie hängen nur von der Länge der Konstellation ab. Für jede einzelne der Konstellationen sind jedoch die Hardy-Littlewood'schen Konstanten spezifisch, und diese möchten wir im Folgenden berechnen.

Zur Erklärung der IF-Abfrage sei noch einmal erwähnt, dass zwei Restklassen $a_i \bmod p$ nur dann zusammenfallen können, wenn zumindest $p \leq a_{max} - a_{min}$ gilt.

```
hardy(a, p_ := 2, r_, s_ := []) :=
  Loop
    If p <= MAX(a) - MIN(a)
       Prog
         r_ := rest(a, p_)
         If DIM(r_) /= DIM(a)
            s_ := APPEND(s_, [[p_, p_ - DIM(r_)]])
         p_ := NEXT_PRIME(p_)
    RETURN s_
```

Als Output erhält man eine Tabelle, die in der ersten Spalte die Primzahlen enthält, und in der zweiten Spalte die Anzahl der freien Restklassen anführt. Dabei werden nur diejenigen Primzahlen aufgelistet, bei denen weniger als $l$ Restklassen besetzt sind. Aus Übersichtsgründen werden jene Zahlen, bei denen genau $l$ Restklassen mod $p$ freibleiben, nicht in der Liste angeführt. Ausgewertet für `riesel`, das Riesel'sche Beispiel, erhält man:

`hardy(riesel)=`

$$\begin{bmatrix} 2 & 1 \\ 3 & 1 \\ 5 & 1 \\ 7 & 1 \\ 11 & 1 \\ 13 & 1 \\ 17 & 4 \\ 19 & 6 \\ 23 & 9 \end{bmatrix}$$

Dies steht im Einklang mit [Rie94]. Auch wenn die Routine bis $p = 53$ rechnet, bleiben ab $p = 29$ jeweils genau $15 = l$ Restklassen frei, weshalb diese Primzahlen im Ergebnisvektor nicht mehr aufscheinen. Wir erhalten also, wenn wir diese Tabelle miteinbeziehen, unmittelbar die Formel (5.15).

Abschließend und unabhängig von den obigen Routinen, soll noch in Anlehnung an die Funktion `NEXT_PRIME` ein Programm entstehen, das zu einer gegebenen Konstellation $a$ und einer Größe $x$ das kleinste Beispiel für die Konstellation $a$ angibt, wobei alle Elemente davon $\geq x$ sind.

```
next_const(x, a, t_) :=
  Loop
    t_ := x - FIRST(a)
    If EVERY(PRIME?(t_ + a_), a_, a)
       RETURN VECTOR(t_ + a_, a_, a)
    x := NEXT_PRIME(x)
```

Natürlich will man sich auch hierbei von der Funktionalität der Routine überzeugen. Als Beispiel könnte man Tripel der Form $[0, 2, 6]$ untersuchen:

```
next_const(190, [0, 2, 6]) = [191, 193, 197]
next_const(191, [0, 2, 6]) = [191, 193, 197]
next_const(192, [0, 2, 6]) = [227, 229, 233]
```

Mit Hilfe von `next_const` können auch ganze Intervalle nach Konstellationen abgesucht werden:

```
noc(x, y, a, i_ := 0, t_) :=
  Loop
    t_ := next_const(x, a)
    If EVERY(j_ <= y, j_, t_)
       i :+ 1
       RETURN i_
    x := FIRST(t_) + 1
```

Somit steht einer genaueren Untersuchung von Konstellationen beliebiger Bauart im Intervall $[x, y]$ nichts mehr im Wege. Es ist klar, dass man etwa durch `noc(1,y,[0,2])` sofort $\pi_2(y)$, die Anzahl der Primzahlzwillinge kleiner oder gleich $y$, erhält.

## 5.4 Konkrete Beispiele von Konstellationen

Mit Hilfe der nunmehr zur Verfügung stehenden Implementierungen lassen sich Primzahlkonstellationen sehr leicht untersuchen. Das größte Handicap stellt wieder einmal der kleine Zahlenumfang dar, der in vernünftiger Zeit mit einem einfachen PC untersucht werden kann. Man kann davon ausgehen, wenigstens bis $y = 10^6$ keinerlei Bedenken haben zu müssen. Aus diesem Grund lassen sich höchstens ältere Tabellen verifizieren, die neueren Werte können auch weiterhin nur zitiert werden (Die Tabellen 5.1 und 5.2 stimmen etwa mit denen aus [Wei99] überein).

Die Primzahlzwillinge $[p, p+2]$ wurden bereits vorgestellt. Es gibt jedoch daneben noch weitere Primzahlkonstellationen, die aus zwei Primzahlen bestehen. Beispielsweise wollen wir die Konstellation

$$[t, t+4] \tag{5.40}$$

betrachten. Die Programme in DERIVE führen ohne Umwege direkt auf die folgende Darstellung

$$P_x(p, p+4) \backsim \frac{2}{1} \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} \int_2^x \frac{dx}{\ln^2 x} = \pi_2(x). \tag{5.41}$$

Wir können somit erwarten, dass es gleichviele herkömmliche Primzahlpaare $(p, p+2)$ gibt, wie Vertreter der Konstellation $[t, t+4]$. Tatsächlich scheint diese Beobachtung durch die Ergebnisse von `noc(x,y,[0,4])` bestätigt zu werden, wie anhand der Tabelle 5.1 ersichtlich ist.

Neben (5.40) betrachten wir noch die Konstellationen

$$[t, t+6] \qquad [t, t+8] \qquad [t, t+10] \qquad [t, t+12]. \tag{5.42}$$

Wieder stellen wir mit unseren Routinen die entsprechenden Berechnungen an, und gelangen so zu den folgenden Abschätzungen

$$P_x(p, p+6) \backsim \frac{2}{1} \frac{2 \cdot 3}{2^2} \prod_{p \geq 5} \frac{p(p-2)}{(p-1)^2} \int_2^x \frac{dx}{\ln^2 x} = 2\pi_2(x), \tag{5.43}$$

$$P_x(p, p+8) \backsim \frac{2}{1} \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} \int_2^x \frac{dx}{\ln^2 x} = \pi_2(x), \tag{5.44}$$

$$P_x(p, p+10) \backsim \frac{2}{1} \frac{3}{2^2} \frac{4 \cdot 5}{4^2} \prod_{p \geq 7} \frac{p(p-2)}{(p-1)^2} \int_2^x \frac{dx}{\ln^2 x} = \frac{4}{3}\pi_2(x), \tag{5.45}$$

$$P_x(p, p+12) \backsim \frac{2}{1} \frac{2 \cdot 3}{2^2} \prod_{p \geq 5} \frac{p(p-2)}{(p-1)^2} \int_2^x \frac{dx}{\ln^2 x} = P_x(p, p+6). \tag{5.46}$$

Da bei der Konstellaton $[t, t+6]$ modulo 3 nur eine Restklasse belegt ist - verglichen mit den Primzahlzwillingen also eine zusätzliche freibleibt - entsteht in (5.43) ein Faktor 2, der bewirkt, dass etwa doppelt soviele Primzahlpaare mit Abstand 6 existieren sollten, als Paare mit Abstand 2 oder 4.

Ähnlich dazu bleibt im Falle von $[t, t+10]$ bei der Primzahl 5 eine Restklasse mehr frei, sodass sich im Vergleich zu $\pi_2(x)$ ein Faktor von $\frac{4}{3}$ ergibt.

Da `hardy([0,6])=hardy([0,12])` gilt, haben schließlich diese beiden Konstellationen approximativ die gleiche Formel, wie ebenfalls aus der Tabelle 5.1 hervorgeht.

| | $(p, p+4)$ | | $(p, p+6)$ | | $(p, p+8)$ | |
|---|---|---|---|---|---|---|
| $n$ | $P_n$ | # | $P_n$ | # | $P_n$ | # |
| $10^3$ | 46 | 41 | 92 | 74 | 46 | 38 |
| $10^4$ | 214 | 203 | 428 | 411 | 214 | 208 |
| $10^5$ | 1.249 | 1.216 | 2.498 | 2.447 | 1.249 | 1.260 |
| $10^6$ | 8.248 | 8.144 | 16.496 | 16.386 | 8.248 | 8.242 |
| $10^7$ | 58.754 | 58.622 | 117.508 | 117.207 | 58.754 | 58.595 |

| | $(p, p+10)$ | | $(p, p+12)$ | |
|---|---|---|---|---|
| $n$ | $P_n$ | # | $P_n$ | # |
| $10^3$ | 61 | 51 | 92 | 69 |
| $10^4$ | 285 | 270 | 428 | 404 |
| $10^5$ | 1.665 | 1.624 | 2.498 | 2.420 |
| $10^6$ | 10.997 | 10.934 | 16.496 | 16.378 |
| $10^7$ | 78.339 | 78.211 | 117.508 | 117.486 |

Tabelle 5.1: Die Anzahl verschiedener Primzahlkonstellationen mit 2 Elementen unterhalb $10^7$. Dabei steht die Vorhersage „$P_n$“ den tatsächlich gezählten „#“ gegenüber.

Neben diversen Paaren von Primzahlen ist es auch naheliegend, sogenannte „Primzahltripel“ zu definieren resp. zu untersuchen. Wie wir schon im Laufe dieses Kapitels festgestellt haben, ist ein Tripel der Bauart $[t, t+2, t+4]$ nicht zulässig, da jeweils eine der drei Zahlen durch drei geteilt werden kann. Es gibt somit keine zulässige Konstellation aus drei Elementen mit $a_l - a_1 = 4$. Setzt man jedoch diese Differenz gleich Sechs, dann ergeben sich folgende zwei Möglichkeiten:

$$[t, t+2, t+6] \qquad \text{bzw.} \qquad [t, t+4, t+6]. \tag{5.47}$$

Von weiteren Beispielen mit drei Elementen soll hier Abstand genommen werden. Stattdessen konzentrieren wir uns auf die Hardy-Littlewood'schen Abschätzungen.

Es stellt sich sehr rasch heraus, dass man wiederum mit zwei identischen Abschätzungen konfrontiert ist. Sowohl bei der Primzahl 2 als auch bei der Primzahl 3 bleibt jeweils eine Restklasse frei, sodass eine Konstante der Form

$$C_3 = \frac{2^2}{1} \cdot \frac{3^2}{2^3} \prod_{p \geq 5} \frac{p^2(p-3)}{(p-1)^3} = \frac{9}{2} \prod_{p \geq 5} \frac{p^2(p-3)}{(p-1)^3} \tag{5.48}$$

resultiert. Somit gelten nach Hardy und Littlewood die folgenden Relationen

$$P_x(p, p+2, p+6) \overset{\mathfrak{L}}{\sim} P_x(p, p+4, p+6) \overset{\mathfrak{L}}{\sim} C_3 \int_2^x \frac{dx}{\ln^3 x} \approx 2.858248596 \int_2^x \frac{dx}{\ln^3 x}. \tag{5.49}$$

Ausgehend von den beiden Tripeln (5.47) lassen sich nun Quadrupel konstruieren, indem man in geeignetem Abstand, also in sozusagen „zulässiger" Art und Weise, eine vierte Zahl an die drei bestehenden anhängt. Auf diesem Wege gelangt man zu folgenden zwei Beispielen für Primzahlquadrupel:

$$[t, t+2, t+6, t+8] \qquad \text{bzw.} \qquad [t, t+4, t+6, t+10]. \tag{5.50}$$

Wieder steuern wir eine Abschätzung der Form

$$C_4 \int_2^x \frac{dx}{\ln^4 x} \tag{5.51}$$

an. Im Fall der Konstellation $[t, t+2, t+6, t+8]$ bleibt für die Primzahlen 2 und 3 jeweils genau eine Restklasse frei, für die übrigen $p$ jeweils $p-4$. So auch für $p = 5$, wo eine Restklasse unbelegt bleibt.

Bei $[t, t+4, t+6, t+10]$ sieht die Lage zunächst ähnlich aus, bleiben doch wieder für 2 und 3 jeweils eine Restklasse frei. Aber für $p = 5$ treten nur die Reste $0, 1$ und 4 auf, es bleiben also die Restklassen 2 und 3 nicht besetzt. Das ist um eine Restklasse mehr, oder anders gesagt: das Doppelte, als bei der ersten Anordnung. Daraus folgt unmittelbar, dass etwa doppelt soviele Primzahlquadrupel der Form $[t, t+4, t+6, t+10]$ unterhalb einer festen Größe existieren, wie Vertreter von $[t, t+2, t+6, t+8]$.

Die Bestimmung von $C_4$ ist nur mehr Formsache, liegen uns doch bereits alle notwendigen Informationen dazu vor (wir ordnen $C_4$ willkürlich $[t, t+2, t+6, t+8]$ zu):

$$C_4 = \frac{2^3}{1^4} \cdot \frac{3^3}{2^4} \prod_{p \geq 5} \frac{p^3(p-4)}{(p-1)^4} = \frac{27}{2} \prod_{p \geq 5} \frac{p^3(p-4)}{(p-1)^4}. \tag{5.52}$$

Nach den Überlegungen vorhin folgt nunmehr:

$$\begin{aligned} P_x(p, p+2, p+6, p+8) &\backsim \frac{1}{2} P_x(p, p+4, p+6, p+10) \backsim \\ &\backsim C_4 \int_2^x \frac{dx}{\ln^4 x} \approx 4.151180864 \int_2^x \frac{dx}{\ln^4 x}. \end{aligned}$$

Abschließend sei noch die zu den letzten vier betrachteten Primzahlkonstellationen dazugehörige Tabelle angeführt:

| | $[0,2,6]$ | | $[0,4,6]$ | | $[0,2,6,8]$ | | $[0,4,6,10]$ | |
|---|---|---|---|---|---|---|---|---|
| $n$ | $P_n$ | # | $P_n$ | # | $P_n$ | # | $P_n$ | # |
| $10^3$ | 26 | 15 | 26 | 15 | 16 | 5 | 32 | 10 |
| $10^4$ | 69 | 57 | 69 | 55 | 24 | 12 | 48 | 25 |
| $10^5$ | 279 | 248 | 279 | 259 | 53 | 38 | 106 | 80 |
| $10^6$ | 1.446 | 1.393 | 1.446 | 1.444 | 184 | 166 | 368 | 317 |

Tabelle 5.2: Die Anzahl verschiedener Primzahltripel und -quadrupel unterhalb $10^6$. Dabei steht die Vorhersage „$P_n$“ den tatsächlich gezählten „#“ gegenüber.

Auch wenn die Schätzungen mit den tatsächlichen Zählergebnissen zum Teil nicht sehr genau übereinzustimmen scheinen, sind manche Vorhersagen über Verhältnisse unter den Konstellationen doch sehr bemerkenswert.

Es gäbe sicherlich noch eine Fülle weiterer Beispiele, die hier angeführt werden könnten. Der Interessierte sei an dieser Stelle jedoch angehalten, die Konstellationen seiner Wahl mit Hilfe der hier vorgestellten einfachen Programme in DERIVE selbst zu untersuchen, und die für ihn interessanten Informationen herauszulesen.

Sollte sich jemand für Statistiken über Konstellationen interessieren, die über den oben abgedeckten Zahlenbereich hinausgehen, sei er etwa auf [JLB67] verwiesen, wo ähnliche Tabellen für Intervalle von $[10^8, 10^8 + 150.000]$ bis $[10^{15}, 10^{15} + 150.000]$ zu finden sind.

Weitere Konstellationen mit bis zu 16 Elementen findet man in dem relativ aktuellen Artikel [For99], wobei jeweils die größten damals bekannten Beispiele aufgelistet sind.

# Anhang A

# DERIVE

## A.1 Verwendete Befehle in DERIVE

Im Folgenden sind die DERIVE-Befehle, die im Zuge dieser Arbeit verwendet wurden, aufgelistet und möglichst kurz in ihrer Funktionalität beschrieben. Man wird dadurch in die Lage versetzt, die Programmzeilen besser zu verstehen und nachvollziehen zu können. Auch soll das Verfassen eigener Programme in DERIVE erleichtert werden.

| Befehl | Ergebnis bzw. kurze Beschreibung |
|---|---|
| `n!` | $n! = 1 \cdot 2 \cdots n$ |
| `#i` | $i = \sqrt{-1}$ |
| `/=` | $\neq$ |
| `k:+1` | der Wert von $k$ wird um 1 erhöht |
| ‘ | Transponieren einer Matrix |
| `ADJOIN(u,v)` | Vektor $v$ mit $u$ an erster Stelle eingefügt |
| `APPEND(v1,v2,...,vn)` | Vektor mit den Elementen von v1 bis vn |
| `APPEND_COLUMNS(s1,s2,...)` | Spalten s1 bis sn zu Matrix zusammengehängt |
| `APPROX(u,n)` | Ausdruck $u$ auf $n$ Stellen genau approximiert |
| `ATAN(x)` | $\arctan(x)$ |
| `BERNOULLI(n)` | $n$te Bernoulli-Zahl $B(n)$ |
| `DELETE_ELEMENT(v,n)` | Vektor $v$ ohne dem $n$ten Element |
| `DIM(v)` | Dimension bzw. Länge des Vektors v |
| `EULER_GAMMA` | gleichnamige Konstante $\gamma$ |

| Befehl | Ergebnis bzw. kurze Beschreibung |
|---|---|
| `EVERY(u,x,c)` | $u(x)$ wird für jedes $x \in c$ ausgewertet. Ist $u(x)$ jedesmal erfüllt, so liefert `EVERY(u,x,c)` *true*, ansonsten *false*. |
| `EXP(x)` | $e^x$ |
| `FALSE` | Boole'sche Konstante „falsch“ |
| `FIRST(v)` | erstes Element im Vektor $v$ |
| `FIT(f,A)` | Liefert nach der Methode der kleinesten Fehlerquadrate eine Annäherung der Form $f$ an die Daten in der Matrix $A$. |
| `FLOOR(x)` | $\lfloor x \rfloor$ |
| `GAMMA(z)` | Gammafunktion $\Gamma(z)$ |
| `INSERT(u,v,n)` | Vektor $v$ mit $u$ an der $n$ten Stelle eingefügt |
| `ITERATE(u,x,x0,xn)` | Iteriert $u(x)$ für $x = x0$ bis $x = xn$ und liefert den letzten Wert zurück |
| `ITERATES(u,x,x0,xn)` | Ähnlich zu `ITERATE(u,x,x0,xn)`, jedoch werden hier sämtliche Zwischenergebnisse in einem Vektor ausgegeben |
| `LN(x)` | $\ln(x)$ |
| `LOG(x,b)` | Logarithmus von $x$ zur Basis $b$: ${}^b\log(x)$ |
| `Loop` | Schleife innerhalb von Programmen (wird mit EXIT oder RETURN verlassen) |
| `MAP_LIST(u,x,c)` | Liste aus $u(x)$ mit $x \in c$ |
| `MAX(x1,x2,...,xn)` | Maximum von $x1, \ldots, xn$ |
| `MEMBER?(u,v)` | „true“ falls $u \in v$, „false“ sonst |
| `MERSENNE_DEGREE(n)` | Exponent von $M_n$ |
| `MIN(x1,x2,...,xn)` | Minimum von $x1, \ldots, xn$ |
| `MOD(m,n)` | $m$ mod $n$ |
| `MOEBIUS_MU(n)` | $\mu(n)$ |
| `NEXT_PRIME(m)` | nächstgrößere Primzahl zu $m$ |
| `NOT` | Boole'scher Operator „nicht“ |
| `NSOLVE(u,x)` | Löst die Gleichung $u(x)$ numerisch nach $x$ auf |
| `NTH_PRIME(n)` | $n$te Primzahl $p_n$ |
| `NUMERATOR(u)` | Zähler des Bruches $u$ |
| `PHASE(z)` | Phasenwinkel einer Komplexen Zahl $z$ |
| `PI` | $\pi$ |
| `PrecisionDigits` | Statusvariable zur Rechengenauigkeit |
| `PRIME(p)` | Liefert zurück, ob $p$ prim ist oder nicht |

| Befehl | Ergebnis bzw. kurze Beschreibung |
|---|---|
| PRIMEPI(x) | $\pi(x)$ |
| PRODUCT(u,n,k,m) | $\prod_{n=k}^{m} u(n)$ |
| Prog | Fasst mehrere Befehle innerhalb von Programmen zusammen |
| RE(z) | Realteil einer komplexen Variablen $z$ |
| REST(v) | Vektor $v$ ohne dem ersten Glied von $v$ |
| RETURN(u) | Beendet eine Routine und liefert $u$ als deren Wert zurück |
| REVERSE(v) | Gespiegelter Vektor von $v$ |
| ROUND(m) | Nächstgelegene ganze Zahl zu $n$ |
| SELECT(u,k,m,n,s) | Vektor mit Elementen für die $u(k)$ erfüllt ist, wobei $k$ von $m$ bis $n$ in Schritten von $s$ läuft |
| SOLVE(u) | Ordnet der Funktion $u$ einen Boole'schen Wahrheitswert zu |
| SORT(l) | Sortiert die Liste $l$ |
| SQRT(z) | $\sqrt{z}$ |
| SQUAREFREE(n) | Überprüft, ob $n$ quadratfrei ist |
| SUB | Referenz auf Index |
| SUM(u,n,k,m) | $\sum_{n=k}^{m} u(n)$ |
| TABLE(u,k,n) | Erzeugt Tabelle mit $n$ Zeilen und 2 Spalten mit $u(k)$, $k = 1, \ldots, n$ |
| TRUE | Boole'sche Konstante „wahr“ |
| VECTOR(u,k,m,n,s) | Vektor mit $u(k)$, $k = m, \ldots, n$ in Abständen von $s$ |
| ZETA(s) | $\zeta(s)$ |

## A.2 Eigene DERIVE-Programme

Hier finden sich die Programme bzw. Konstanten aufgelistet, die im Zuge dieser Arbeit besprochen wurden. Überdies wird die Seite angeführt, auf welcher der entsprechende Source-Code nachgelesen werden kann.

| Name | Erklärung | Seite |
|---|---|---|
| `admissible(a)` | Überprüft, ob die Konstellation `a` zulässig ist | 118 |
| `EI(x,m)` | $\mathrm{ei}(x)$ unter Zuhilfenahme der ersten $m$ Reihenglieder in $\mathrm{ei}(x) = \ln(x)+\gamma+\sum_{n=1}^{\infty} \frac{x^n}{n \cdot n!}$ | 64 |
| `eire(x)` | $\mathrm{Re}(\mathrm{ei}(x))$ mit optimaler Wahl des $m$ aus `EI(x,m)` | 65 |
| `f10(x)` | $\Phi(x, 10)$ | 91 |
| `ff(x,a)` | $\Phi(x, a)$ mit fester Rekursionstiefe | 91 |
| `fortune(n)` | $n$te Fortune'sche Zahl | 38 |
| `free(a,p)` | Überprüft, ob im Vektor $a$ mod $p$ eine Restklasse mod $p$ frei bleibt | 117 |
| `hardy(a)` | Gibt die Primzahlen und die dazugehörige Anzahl freier Restklassen aus, die zur Erstellung der Hardy-Littlewood'schen Konstanten benötigt werden | 119 |
| `ip(x,d,o,l)` | Bestimmung des Wertes von $\pi(x)$ durch Interpolation. `o` ist Steuerungsparameter, `l` eine Liste mit Werten, die in Abständen `d` berechnet wurden | 89 |
| `ip1(x,p,s)` | Zählt $\pi(x) - p$ zu $s$ hinzu | 88 |
| `ip2(x,p,s)` | Zieht $p - \pi(x)$ von $s$ ab | 89 |
| `leg(x,k)` | Berechnet $\pi(x)$ nach Legendre | 73 |
| `legendre(x)` | Berechnet $\pi(x)$ nach Legendre, rekursiv | 78 |
| `meissel(x)` | Berechnet $\pi(x)$ nach Meissel | 79 |
| `mupos` | Positionen, wo $\mu(n) \neq 0$ ist | 67 |
| `muval` | an den Stellen von `mupos` die Werte $-2\frac{\mu(n)}{n}$ | 67 |
| `next_const(x,a)` | zu `x` nächstgrößere Konstellation vom Typ `a` | 120 |
| `next_germain(n)` | Gibt zu $n$ das nächstgrößere Paar von Sophie Germain Primzahlen aus | 32 |
| `next_wieferich(n)` | Berechnet zu $n$ die nächstgrößere Wieferich'sche Primzahl | 34 |

| Name | Erklärung | Seite |
|---|---|---|
| `next_wilson(n)` | Berechnet zu $n$ die nächstgrößere Wilson'sche Primzahl | 35 |
| `noc(x,y,a)` | Zählt Konstellationen $a$ zwischen $x$ und $y$ | 120 |
| `noel(a)` | gibt an, welches Element von $a$ wie oft vorkommt | 38 |
| `nog(n)` | Anzahl der Sophie Germain Primzahlen unterhalb von $n$ | 32 |
| `nopp(n,m)` | Anzahl der primen Primorials im Intervall $[m, n]$ | 36 |
| `nprime(n)` | $n$te Primzahl mit Hilfe von eigenem `primepi(x)` | 92 |
| `NTH_PRIME(n)` | eingebaute Routine für $n$te Primzahl | 91 |
| `P(x,k,a)` | Berechnet die Größe $P_k(x, a)$ | 90 |
| `Phi(x,a)` | Berechnet $\Phi(x, a)$ | 78 |
| `pi_null(x,k)` | Stellt $\pi_0(x)$ als $R^+(x)$ plus Korrekturterme der ersten $k$ kopmlexen Nullstellen von $\zeta(s)$ dar | 70 |
| `piht(x)` | $\pi(x)$ für $1.000 < x \leq 100.000$ durch `ip(x,d,o,l)` | 89 |
| `pim(x)` | $\pi(x)$ für $100.000 < x \leq 1.000.000$ durch `ip(x,d,o,l)` | 89 |
| `pit(x)` | $\pi(x)$ für $x \leq 1.000$ durch `ip(x,d,o,l)` | 89 |
| `pizm(x)` | $\pi(x)$ für $1.000.000 < x \leq 10.000.000$ durch `ip(x,d,o,l)` | 89 |
| `ppi(x,s)` | Berechnet die Anzahl der Primzahlen zwischen $s$ und $x$: $s < p \leq x$ | 87 |
| `prev_prime(x)` | die zu $x$ vorhergehende Primzahl | 88 |
| `primepi(x)` | $\pi(x)$, Anzahl der Primzahlen $\leq x$ | 90 |
| `primorial(n)` | Berechnet $n$tes Primorial $n\#$ | 36 |
| `prod(a)` | Berechnet aus der $m \times n$-Matrix alle möglichen Produkte, die genau $m$ Faktoren aus je einer Zeile aufweisen - für direkte Variante von $\pi(x)$ nach Legendre | 73 |
| `r_h` | Hilfsgröße zur Riemann'schen Funktion $R(x)$ | 61 |
| `riemann(x)` | Riemann'schen Funktion $R(x)$ | 61 |
| `riemannsiegelz(t)` | Riemann-Siegel Funktion $Z(t)$ | 53 |
| `riesel` | Konstellation von Riesel, (5.14) | 118 |
| `rplus(x)` | $R^+(x)$ | 64 |

| Name | Erklärung | Seite |
|---|---|---|
| `regular(p)` | Überprüft, ob $p$ eine reguläre Primzahl ist | 30 |
| `rest(a,p)` | liefert die einzelnen belegten Restklassen von $a$ mod $p$ zurück, ohne deren Vielfachheit | 118 |
| `sel(x,k,a)` | Ermittelt die Primzahlen, die man braucht, um $P_k(x,a)$ zu berechnen | 90 |
| `setmu(m)` | Belegt die globalen Variablen `mupos` und `muval` bis $m$ | 68 |
| `smallpi(x)` | Vorstufe zu `primepi(x)` | 89 |
| `T(x,k)` | Korrekturterm für $\pi(x)$ zur $k$ten komplexen Nullstelle von $\zeta(s)$ | 68 |
| `Tmu(x,k)` | Berechnet die notwendigen Werte von $\mathrm{Re}\left[\mathrm{ei}\left(\frac{\varrho_n}{n}\ln x\right)\right]$ für die Berechnug von $T_k(x)$ | 68 |
| `wprim(n)` | Wahrscheinlichkeit, dass $n$ prim ist | 10 |
| `zetaZeros` | Imaginärteile der komplexen Nullstellen von $\zeta(s)$: $\rho_k = \frac{1}{2} \pm i\alpha_k$ | 53 |

# Danksagung

Wie schon das Sprichwort „Der Erfolg hat viele Väter“ sagt, sind auch am Gelingen dieser Arbeit zahlreiche Helfer beteiligt, denen ich zu besonderem Dank verpflichtet bin.

Zu allererst möchte ich Herrn Prof. Wiesenbauer meinen aufrichtigen Dank zum Ausdruck bringen. Er war sofort bereit, mir beim Thema der Diplomarbeit entgegenzukommen, und machte es somit möglich, eine Arbeit auf meinem Lieblingsgebiet zu verfassen. Das eigene Interesse am „Forschungsbereich“ ist sicherlich ein wichtiger Schritt in Richtung einer zufriedenstellenden Lösung der gestellten Aufgaben.

Zum anderen hatte er auch jederzeit ein offenes Ohr, wenn ich - zeitweise beinahe wöchentlich - seine kostbare Zeit in Anspruch nahm, um ihn mit dem einen oder anderen Problem zu konfrontieren. Nicht zuletzt seine fundierten Kenntnisse des Computeralgebrasystems DERIVE waren immer wieder ausschlaggebend dafür, dass ich ihn aufsuchte. Einerseits half er mir, die benötigten Programme in DERIVE zu perfektionieren, und andererseits brachte er mir, seinem Leitsatz „learning by doing“ folgend, immer wieder theoretische Überlegungen näher.

Weiters möchte ich mich bei meiner Familie bedanken. Meine Eltern, vor allem mein Vater, halfen in oft mühevoller und zeitaufwendiger Arbeit mit, so manchen stilistischen Fehler aus dem Text zu verbannen.

Auch mein Bruder unterstützte mich bei der Korrektur, wofür ich ihm ebenfalls herzlich danke.

Last but not least sei mein Studienkollege und Freund Andreas Traxler bedankt. Vor allem beim abschließenden Korrigieren dieser Arbeit und bei zahlreichen Problemen die Feinabstimmung in LaTeX betreffend gab er mir nützliche Tipps.

# Lebenslauf

## Persönliche Daten

| | |
|---|---|
| Vorname: | Georg |
| Familienname: | GUTENBRUNNER |
| geboren am | 15.11.1978 in Linz |
| Adressen: | Greinerstraße 21, 4320 Perg |
| | Breitenfeldergasse 9/17, 1080 Wien |

## Bildungsgang

| | |
|---|---|
| 1985-1989 | Besuch der Volksschule in Perg |
| 1989-1993 | Besuch der Hauptschule I in Perg, 1. Leistungsstufen |
| 1993-1997 | Bundesoberstufenrealgymnasium Perg, naturwissenschaftlicher Zweig mit Darstellender Geometrie |
| Juni 1997 | Matura mit ausgezeichnetem Erfolg<br>Fachbereichsarbeit in Mathematik mit dem Titel „Zahlentheoretische Spielereien“ |
| Oktober 1997 | Immatrikulation an der Technischen Universität Wien<br>Technische Mathematik der Computerwissenschaften |
| Juli 1999 | Industriepraktikum bei der Firma Siemens AG |
| Oktober 1999 | Beginn des Zweitstudiums Wirtschaftsinformatik an der Universität Wien |
| März 2000 | Praktikum am Institut für Numerische und Angewandte Mathematik der Technischen Universität Wien (E115) |
| Juli 2000 | Praktikum am Institut für Biomedizinische Technik und Physik des AKH Wien |
| Oktober 2000 | Studienassistent am Institut E115 der TU Wien |
| März 2001 | Studienassistent am Institut für Softwarewissenschaft der Universität Wien |
| Juni 2001 | Beginn der Diplomarbeit am Institut für Algebra und Computermathematik der Technischen Universität Wien |
| Oktober 2001 | Studienassistent am Institut E115 der TU Wien |
| März 2002 | Studienassistent am Institut E115 der TU Wien |

# Literaturverzeichnis


[AZ01] Aigner, Martin und Günter M. Ziegler: *Proofs from THE BOOK*. Springer-Verlag, Berlin Heidelberg, zweite Auflage, 2001.

[BCDVH00] Brent, R.P., R.E. Crandall, K. Dilcher und C. Van Halewyn: *Three new factors of Fermat numbers*. Math. Comp., 69(231):1297–1304, 2000. elektronisch veröffentlicht am 1. März 2000.

[BCP82] Buhler, J.P., R.E. Crandall und M.A. Penk: *Primes of the Form $n!\pm 1$ and $2\cdot 3\cdot 5\cdots p\pm 1$*. Math. Comp., 38(158):639–643, April 1982.

[BCS92] Buhler, J.P., R.E. Crandall und R.W. Sompolski: *Irregular primes to one million*. Math. Comp., 59(200):717–722, Oktober 1992.

[BH78a] Bays, Carter und Richard H. Hudson: *Details of the first region of integers $x$ with $\pi_{3,2}(x) < \pi_{3,1}(x)$*. Math. Comp., 32(142):571–576, April 1978.

[BH78b] Bays, Carter und Richard H. Hudson: *On the fluctuations of Littlewood for primes of the form $4n \pm 1$*. Math. Comp., 32(141):281–286, Januar 1978.

[BH99] Bays, Carter und Richard H. Hudson: *A new bound for the smallest $x$ with $\pi(x) > \mathrm{li}(x)$*. Math. Comp., 69(231):1285–1296, 1999. elektronisch veröffentlicht am 4. Mai 1999.

[BLRW82] Brent, R.P., J. van de Lune, H.J.J. te Riele und D.T. Winter: *On the zeros of the Riemann zeta function in the critical strip. II*. Math. Comp., 39(160):681–688, Oktober 1982.

[Boh72] Bohman, Jan: *On the number of primes less than a given limit*. BIT, 12:576–577, 1972.

[Bor72] Borning, Alan: *Some Results for $k! \pm 1$ and $2 \cdot 3 \cdot 5 \cdots p \pm 1$.* Math. Comp., 26(118):567–570, April 1972.

[BP81] Brent, Richard P. und John M. Pollard: *Factorization of the eighth Fermat number.* Math. Comp., 36(154):627–630, 181.

[Bre75] Brent, Richard P.: *Irregularities in the distribution of primes and twin primes.* Math. Comp., 29(129):43–56, Januar 1975. Corrigendum: Math. Comp., 30:198, 1976.

[Bre79] Brent, Richard P.: *On the zeros of the Riemann zeta function in the critical strip.* Math. Comp., 33(148):1361–1372, Oktober 1979.

[Bre99] Brent, Richard P.: *Factorization of the $F_{10}$.* Math. Comp., 68(225):429–451, Januar 1999.

[BS96] Bach, Eric und Jeffrey Shallit: *Algorithmic Number Theory, Volume I: Efficient Algorithms.* Foundations of Computing. The MIT Press, Cambridge, erste Auflage, 1996.

[BSWJ89] Bateman, P.T., J.L. Selfridge und S.S. Wagstaff Jr.: *The new Mersenne conjecture.* Amer. Math. Monthly, 96:125–128, Februar 1989.

[Cal95] Caldwell, Chris K.: *On the primality of $n! \pm 1$ and $2 \cdot 3 \cdot 5 \cdots p \pm 1$.* Math. Comp., 64(210):889–890, April 1995.

[CDNY95] Crandall, R., J. Doenias, C. Norrie und J. Young: *The twenty-second Fermat number is composite.* Math. Comp., 64(210):863–868, April 1995.

[CDP97] Crandall, Richard, Karl Dilcher und Carl Pomerance: *A Search fpr Wieferich and Wilson Primes.* Math. Comp., 66(217):433–449, Januar 1997.

[CP79] Crandall, R.E. und M.A. Penk: *A Search for Large Twin Prime Pairs.* Math. Comp., 33(145):383–388, Januar 1979.

[CP01] Crandall, Richard und Carl Pomerance: *Prime numbers - A computational perspective.* Springer-Verlag, New York, 2001.

[Cra91] Crandall, Richard E.: *Mathematica for the Sciences.* Addison-Wesley, Redwood City, CA, erste Auflage, 1991.

[Cra94] Crandall, Richard E.: *Projects in Scientific Computation.* Springer Verlag New York, Inc., Ney York, erste Auflage, 1994.

[Cra96] Crandall, Richard E.: *Topics in Advanced Scientific Computation.* Springer Verlag New York, Inc., New York, erste Auflage, 1996.

[CW80] Cormack, G.V. und H.C. Williams: *Some very large primes of the form $k \cdot 2^m + 1$.* Math. Comp., 35(152):1419–1421, Oktober 1980.

[CWJ91] Colquitt, W.N. und L. Welsh Jr.: *A new Mersenne prime.* Math. Comp., 56(194):867–870, April 1991.

[Dia82] Diamond, Harold G.: *Elementary methods in the study of the distribution of prime numbers.* Bull. Amer. Math. Soc., 7(3):551–589, 1982.

[DN97] Dubner, Harvey und Harry Nelson: *Seven Consecutive Primes in Arithmetic Progression.* Math. Comp., 66(220):1743–1749, Oktober 1997.

[DR96] Deleglise, M. und J. Rivat: *Computing $\pi(x)$: the Meissel, Lehmer, Lagarias, Miller, Odlyzko method.* Math. Comp., 65(213):235–245, Januar 1996.

[DR98] Deleglise, Marc und Joel Rivat: *Computing $\psi(x)$.* Math. Comp., 67(224):1691–1696, Oktober 1998.

[Dub] Dubner, Harvey: *Repunit $R49081$ is a probable Prime.* Math. Comp., Seiten 1–3. elektronisch veröffentlicht am 30. März 2001.

[Dub87] Dubner, Harvey: *Factorial and Primorial Primes.* J. Recreational Math., 19:197–203, 1987.

[Dub93] Dubner, Harvey: *Generalized Repunit primes.* Math. Comp., 61(204):927–930, Oktober 1993.

[Dub96] Dubner, Harvey: *Large Sophie Germain Primes.* Math. Comp., 65(213):393–396, Januar 1996.

[Dud69] DUDLEY, UNDERWOOD: *History of a formula for primes.* Amer. Math. Monthly, 76:23–28, Januar 1969.

[Dus99] DUSART, PIERRE: *The $k^{th}$ prime is greater than $k(\ln k + \ln\ln k - 1)$ for $k \geq 2$.* Math. Comp., 68(225):411–415, Januar 1999.

[Ehr67] EHRMAN, JOHN R.: *The number of prime divisors of certain Mersenne numbers.* Math. Comp., 21:700–704, 1967.

[Ewi92] EWING, J.: *The latest Mersenne prime.* Amer. Math. Monthly, 99:360, April 1992.

[Ewi94] EWING, J.: $2^{858433} - 1$ *is prime.* Amer. Math. Monthly, 101:338, April 1994.

[For97] FORBES, TONY: *A Large Pair of Twin Primes.* Math. Comp., 66(217):451–455, Januar 1997.

[For99] FORBES, TONY: *Prime Clusters and Cunningham Chains.* Math. Comp., 68(228):1739–1747, 1999. elektronisch veröffentlicht am 24. Mai 1999.

[Frü50] FRÜCHTL, KURT: *Statistische Untersuchung über die Verteilung von Primzahl-Zwillingen.* Anz. Österr. Akad. Wiss., 87:226–232, 1950.

[Gil64] GILLIES, DONALD B.: *Three new Mersenne primes and statistical theory.* Math. Comp., 18:93–97, 1964.

[Gol81] GOLOMB, SOLOMON W.: *The Evidence for Fortune's Conjecture.* Math. Mag., 54(4):209–210, September 1981.

[Gro82] GROSSWALD, E.: *Arithmetic progressions that consist only of primes.* Journal of Number Theory, 14:9–31, 1982.

[Guy94] GUY, RICHARD K.: *Unsolved Problems in Number Theory*, Band 1 der Reihe *Problem Books in Mathematics: Unsolved Problems in Intuitive Mathematics.* Springer-Verlag, New York, zweite Auflage, 1994.

[Guy98] GUY, RICHARD K.: *Nothing's new in number theory?* Amer. Math. Monthly, 105:951–954, Dezember 1998.

[HJC98] Hagis Jr., Peter und Graeme L. Cohen: *Every odd perfect number has a prime factor which exceeds* $10^6$. Math. Comp., 67(223):1323–1330, Juli 1998.

[HL22] Hardy, G.H. und J.E. Littlewood: *Some problems of 'Partitio numerorum' III: On the expression of a number as a sum of primes.* Acta. Math., (44):1–70, 1922.

[HS79] Hlawka, Edmund und Johannes Schoissengeier: *Zahlentheorie, eine Einführung.* Manzsche Verlags- und Universitätsbuchhandlung, Wien, 1979.

[HW58] Hardy, G.H. und E.M. Wright: *Einführung in die Zahlentheorie.* R. Oldenbourg, München, dritte Auflage, 1958.

[Ian99a] Iannucci, Douglas E.: *The second largest prime divisor of an odd perfect number exceeds ten thousand.* Math. Comp., 68(228):1749–1760, 1999.

[Ian99b] Iannucci, Douglas E.: *The third largest prime divisor of an odd perfect number exceeds one hundred.* Math. Comp., 69(230):867–879, 1999.

[IJ96] Indlekofer, Karl-Heinz und Antal Jarai: *Largest known twin primes.* Math. Comp., 65(213):427–428, Januar 1996.

[IJ99] Indlekofer, Karl-Heinz und Antal Jarai: *Largest known twin primes and Sophie Germain primes.* Math. Comp., 68(227):1317–1324, 1999. elektronisch veröffentlicht am 16. Februar 1999.

[JLB67] Jones, M.F., M. Lal und W.J. Blundon: *Statistics on Certain Large Primes.* Math. Comp., 21:103–107, 1967.

[Joh75] Johnson, Wells: *Irregular Primes and Cyclotomic Invariants.* Math. Comp., 29(129):113–120, Januar 1975.

[Kel83] Keller, Wilfrid: *Corrigendum zu „Primes of the form* $n! \pm 1$ *and* $2 \cdot 3 \cdot 5 \cdots p \pm 1$*“.* Math. Comp., 40:727, 1983.

[Kel95] Keller, Wilfrid: *New Cullen primes.* Math. Comp., 64(212):1733–1741, Oktober 1995.

[Knö51] Knödel, Walter: *Sätze über Primzahlen I.* Mh. Math., (55):62–75, 1951.

[Knö52] Knödel, Walter: *Sätze über Primzahlen II.* Mh. Math., (56):137–143, 1952.

[Lan09a] Landau, Edmund: *Handbuch der Lehre von der Verteilung der Primzahlen*, Band 1. B.G.Teubner, Leipzig, erste Auflage, 1909.

[Lan09b] Landau, Edmund: *Handbuch der Lehre von der Verteilung der Primzahlen*, Band 2. B.G.Teubner, Leipzig, erste Auflage, 1909.

[LMO85] Lagarias, J.C., V.S. Miller und A.M. Odlyzko: *Computing $\pi(x)$: The Meissel-Lehmer Method.* Math. Comp., 44(170):537–560, April 1985.

[LO87] Lagarias, J.C. und A.M. Odlyzko: *Computing $\pi(x)$: an analytic method.* J. Algorithms, 8:173–191, 1987.

[LP67] Lander, L.J. und T.R. Parkin: *Consecutive primes in arithmetic progression.* Math. Comp., 21:489, 1967.

[LR83] Lune, J. van de und H.J.J. te Riele: *On the zeros of the Riemann zeta function in the critical strip. III.* Math. Comp., 41(164):759–767, Oktober 1983.

[LRW86] Lune, J. van de, H.J.J. te Riele und D.T. Winter: *On the zeros of the Riemann zeta function in the critical strip. IV.* Math. Comp., 46(174):667–681, April 1986.

[Map63] Mapes, David C.: *Fast Method for Computing the Number of Primes Less than a Given Limit.* Math. Comp., 17:179–185, 1963.

[Mei70] Meissel, E.D.F.: *Über die Bestimmung der Primzahlmenge innerhalb gegebener Grenzen.* Math. Ann., 2:636–642, 1870.

[Mei71] Meissel, E.D.F.: *Berechnung der Menge von Primzahlen, welche innerhalb der ersten Hundert Millionen natürlicher Zahlen vorkommen.* Math. AnN., 3:523–525, 1871.

[Mei83] Meissel, E.D.F.: *Über Primzahlmengen.* Math. Ann., 21:304, 1883.

[Mei85] Meissel, E.D.F.: *Berechnung der Menge von Primzahlen, welche innerhalb der ersten Milliarde natürlicher Zahlen vorkommen.* Math. Ann., 25:251–257, 1885.

[Mil47] Mills, W.H.: *A prime-representing function.* Bull. Amer. Math. Soc., 53:604, 1947.

[Mor93] Moree, P.: *Betrand's Postulate for Primes in Arithmetical Progressions.* Computers Math. Appl., 26(5):35–43, 1993.

[MR96] Massias, J.-P. und G. Robin: *Bornes effectives pour certaines fonctions concernant les nombres premiers.* J. Th. N. Bordeaux, 8:215–242, 1996.

[New80] Newman, D.J.: *Simple analytic proof of the prime number theorem.* Amer. Math. Monthly, Seiten 693–696, November 1980.

[Nic95] Nicely, Thomas R.: *Enumeration to* $10^{14}$ *of the twin primes and Brun's constant.* Virginia Journal of Science, Seiten 195–204, 1995.

[NZ76] Niven, Ivan und Herbert S. Zuckerman: *Einführung in die Zahlentheorie I + II*, Band 46 + 47 der Reihe *Hochschultaschenbuch.* B.I.-Wissenschaftsverlag, Mannheim, erste Auflage, 1976.

[PMT95] Pritchard, Paul A., Andrew Moran und Anthony Thyssen: *Twenty-two primes in arithmetic progression.* Math. Comp., 64(211):1337–1339, Juli 1995.

[Pra57] Prachar, Karl: *Primzahlverteilung*, Band XCI der Reihe *Die Grundlehren der Mathematischen Wissenschaften in Einzeldarstellungen.* Springer-Verlag, Berlin, erste Auflage, 1957.

[PSZ90] Parady, B.K., Joel F. Smith und Sergio E. Zarantonello: *Largest known twin primes.* Math. Comp., 55(191):381–382, Juli 1990.

[RG70] Riesel, Hans und Gunnar Göhl: *Some Calculations Related to Riemann's Prime Number Formula.* Math. Comp., 24(112):969–983, Oktober 1970.

[Rib79] Ribenboim, Paulo: *13 Lectures on Fermat's Last Theorem.* Springer-Verlag, New York, 1979.

[Rib96] Ribenboim, Paulo: *The New Book of Prime Number Records.* Springer-Verlag, dritte Auflage, 1996.

[Ric74] Richards, Ian: *On the incompatibility of two conjectures concerning primes.* Bull. Amer. Math. Soc., 80:419–438, 1974.

[Rie59] Riemann, Bernhard G.F.: *Über die Anzahl der Primzahlen unter einer gegebenen Größe.* Monatsberichte der Berliner Akademie, Seiten 136–144, 1859.

[Rie87] Riele, Hermann J.J. te: *On the Sign of the Difference* $\pi(x) - \mathrm{li}(x)$. Math. Comp., 48(177):323–328, Januar 1987.

[Rie94] Riesel, Hans: *Prime Numbers and Computer Methods for Factorization*, Band 126 der Reihe *Progress in mathematics.* Birkhäuser Verlag, Boston, zweite Auflage, 1994.

[Rob83] Robin, G.: *Estimation de la fonction de Tchebychef* $\theta$ *sur k-ime nombre premier et grandes valeurs de la fonctions* $\omega(n)$*, nombre de diviseurs premiers de* $n$. Acta Arithmetica, 42(4):367–389, 1983.

[Ros39] Rosser, J. B.: *The n-th prime is greater than* $n \log n$. Proc. London Math. Soc., 45(2):21–44, 1939.

[Sch83] Schroeder, Manfred R.: *Where Is the Next Mersenne Prime Hiding?* Math. Int., 5(3):31–33, 1983.

[Sel49] Selberg, Atle: *An elementary proof of the prime-number theorem.* Math. Ann., 50(2):305–313, April 1949.

[SH64] Selfridge, J.L. und Alexander Hurwitz: *Fermat numbers and Mersenne numbers.* Math. Comp., 18:146–148, 1964.

[Spe56] Specht, Wilhelm: *Elementare Beweise der Primzahlsätze*, Band 30 der Reihe *Hochschulbücher für Mathematik.* VEB Deutscher Verlag der Wissenschaften, Berlin, 1956.

[SW74] Shanks, Daniel und John W. Wrench: *Brun's Constant.* Math. Comp., 28(125):293–299, 1974.

[Tem80] Templer, Mark: *On the Primality of* $k!+1$ *and* $2 \cdot 3 \cdot 5 \cdots p \pm 1$. Math. Comp., 34(149):303–304, Januar 1980.

[Tro53] Trost, Ernst: *Primzahlen*, Band 2 der Reihe *Elemente der Mathematik vom höheren Standpunkt aus.* Birkhäuser Verlag, Basel, erste Auflage, 1953.

[Var91] VARDI, ILAN: *Computational Recreations in Mathematica*. Addison-Wesley, Redwood City, CA, erste Auflage, 1991.

[VE80] VANDEN EYNDEN, CHARLES: *Proofs the* $\sum 1/p$ *diverges*. Amer. Math. Monthly, 87:394–397, Mai 1980.

[Veh79] VEHKA, THOMAS: *Explicit construction of an admissible set for the conjecture that sometimes* $\pi(x+y) > \pi(y) + \pi(x)$. Not. Amer. Math. Soc., 26:A–453, 1979.

[Wag78] WAGSTAFF, SAMUEL S.: *The irregular primes to* 125000. Math. Comp., 32(142):583–591, April 1978.

[Wag99] WAGON, STAN: *Mathematica in action*. Springer-Verlag, New York, zweite Auflage, 1999.

[Wei99] WEISSSTEIN, ERIC: *CRC Concise Encyclopedia of Mathematics*. CRC Press, London-New York-Washington, erste Auflage, 1999.

[Wie97] WIESENBAUER, JOHANN: *Abzählen von Primzahlen mit DERIVE*. Österreichische Mathematische Gesellschaft: Schriftreihe zur Didaktik der Mathematik der Höheren Schulen, Heft 27:196–206, November 1997.

[Wil93] WILLIAMS, H.C.: *How was* $F_6$ *factored?* Math. Comp., 61(203):463–474, Juli 1993.

[YB88] YOUNG, JEFF und DUNCAN A. BUELL: *The twentieth Fermat number is composite*. Math. Comp., 50(181):261–263, Januar 1988.

[You98] YOUNG, JEFF: *Large primes and Fermat factors*. Math. Comp., 67(224):1735–1738, Oktober 1998.

[Zag77] ZAGIER, DON: *The first 50 million prime numbers*. Math. Intelligencer, 0:7–19, 1977.

# Web-Literaturverzeichnis


[1] Alfeld, P.: *„Understanding Mathematics“*
http://www.math.utah.edu/∼alfeld/math/mersenne.html/

[2] Caldwell, C. : *Website für Primzahlen.*
http://primes.utm.edu/

[3] Caldwell, C.: *„How many primes are there?“*
http://primes.utm.edu/howmany/

[4] Caldwell, C.: *Die größten bekannte Primzahlen*
http://primes.utm.edu/largest/

[5] Caldwell, C.: *„The Top Twenty Lists“*
http://primes.utm.edu/lists/top20/

[6] Caldwell, C.: *Mersenne'sche Zahlen*
http://primes.utm.edu/mersenne/

[7] Crandall, R., E. Mayer und J. Papadopoulos: *The twenty-fourth Fermat number is composite*
http://www.perfsci.com/

[8] Crandall, R.: *Perfectly Scientific, Inc. prize page*
http://www.perfsci.com/prizes.html/

[9] Durman, L.: *Districuted Search for Fermat Number Divisors*
http://www.fermatsearch.org/

[10] Faber and Faber Publishing Company: *$1.000.000 challenge to prove Goldbach's conjecture*
http://www.faber.co.uk/faber/million_dollar.asp/

[11] Finch, S.: *„Mathsoft Constants“: Mathematische Konstanten*
http://www.mathcad.com/library/constants/

[12] Finkelstein, S.: *Electronic Frontier Foundation*
http://www.eff.org/awards/prime-info.html

[13] Forbes, T.: *Prime k-tuplets*
http://www.ltkz.demon.co.uk/ktuplets.htm/

[14] Forster, O.: *Bilder von Primzahlen*
http://www.mathematik.uni-muenchen.de/~forster/primes.html/

[15] Hartmann, P.: *Beweise des Satzes von Euklid*
http://www.beweise.mathematic.de/

[16] Hartmann, P.: *Zahlenarten in der Mathematik*
http://www.zahlen.mathematic.de/

[17] Jonietz, A.: *Wundersame Zahlen & Co*
http://www.jonietz.de/jufo/wundersam/jufo99.html/

[18] Keller, W.: *Prime factors $k \cdot 2^n + 1$ of Fermat numbers $F_m$ and complete factoring status*
http://www.prothsearch.net/fermat.html/

[19] Nicely, T.: *Enumeration to $1.6 \times 10^{15}$ of the twin primes and Brun's constant*
http://www.trnicely.net/twins/twins2.html/

[20] O'Connor, J.J. und E.F. Robertson: *Geschichte der Primzahlen*
http://www-groups.dcs.st-and.ac.uk/~history/HistTopics/Prime_numbers.html/

[21] Odlyzko, A.: *The $10^{20}$-th zero of the Riemann zeta function and 175 million of its neighbors*
http://www.dtc.umn.edu/~odlyzko/

[22] Rivera, C.: *The primepuzzles & problems connection*
http://www.primepuzzles.net/

[23] Sloane, N.J.A.: *The Online Encyclopedia of Integer Sequences*
http://www.research.att.com/~njas/sequences/index.html/

[24] Weissstein, E.: *World of mathematics*
http://mathworld.wolfram.com/

[25] Woltman, G.: *Great Internet Mersenne prime search (GIMPS)*
http://www.mersenne.org/

[26] *American Mathematical Society*
`http://www.ams.org/`

[27] *Die deutsche Primzahlseite*
`http://www.primzahlen.de/`

[28] *MegaNumbers: The Software Tools Team's Prime Number and Very Large Integer R & D Web site*
`http://www.meganumbers.com/`

[29] *Zentralblatt MATH*
`http://www.emis.de/ZMATH/`

# Index