4
Wie sind die Primzahlen verteilt?

Wie ich bereits betont hatte, sind die verschiedenen Beweise der Unendlichkeit der Anzahl der Primzahlen nicht konstruktiv. Man erhält daher keine Aussage darüber, wie man die n-te Primzahl bestimmen kann. Zudem geben die Beweise auch keinen Hinweis darauf, wie viele Primzahlen es bis zu einer vorgegebenen Zahl N gibt. Und umgekehrt ist keine vernünftige Formel oder Funktion bekannt, die die Primzahlen repräsentiert.

Es ist jedoch möglich, die Anzahl der Primzahlen kleiner als N mit einer recht hohen Genauigkeit vorauszusagen (vor allem für großes N). Jedoch weist die Verteilung der Primzahlen in kleinen Intervallen eine Art eingebaute Zufälligkeit auf. Diese Kombination von gleichzeitiger „Voraussagbarkeit“ und „Zufälligkeit“ bedeutet einerseits eine systematische Ordnung, andererseits ein Überraschungselement bei der Verteilung der Primzahlen. Laut Schroeders faszinierendem Buch *Number Theory in Science and Communication* sind dies grundlegende Bestandteile von Kunst. Und viele Mathematiker würden sofort zustimmen, dass dieses Thema von großem ästhetischen Reiz ist.

Man erinnere sich aus Kapitel 3, dass für jede reelle Zahl $x > 0$ durch $\pi(x)$ die Anzahl der Primzahlen p mit $p \leq x$ ausgedrückt ist; man nennt $\pi(x)$ auch die *Primzahlfunktion*.

P. Ribenboim, *Die Welt der Primzahlen*, 2. Aufl., Springer-Lehrbuch,
DOI 10.1007/978-3-642-18079-8_4, © Springer-Verlag Berlin Heidelberg 2011

Die folgenden Themen werden behandelt:

(I) Eigenschaften von $\pi(x)$: das Wachstum von $\pi(x)$, die Größenordnung sowie Vergleiche mit anderen bekannten Funktionen.

(II) Ergebnisse über die n-te Primzahl sowie zur Differenz zwischen aufeinander folgenden Primzahlen, wie klein, wie groß und wie unregelmäßig sie sein kann. Dies beinhaltet die Diskussion von großen Primzahllücken und führt zudem auf einige offene Probleme, die weiter unten angesprochen werden.

(III) Primzahlzwillinge, ihre Charakterisierung und Verteilung.

(IV) Primzahlmehrlinge.

(V) Primzahlen in arithmetischen Folgen.

(VI) Goldbachs berühmte Vermutung.

(VII) Die Verteilung der Pseudoprimzahlen und Carmichael-Zahlen.

Nun zu den einzelnen Punkten.

I Die Funktion $\pi(x)$

Die grundlegende Idee beim Studium von $\pi(x)$ oder verwandter Funktionen in Bezug auf die Primzahlverteilung ist der Vergleich mit klassischen, einfach berechenbaren Funktionen, deren Werte so nah wie möglich bei $\pi(x)$ liegen sollten. Dies ist natürlich nicht einfach und wie man vielleicht erwarten könnte, wird auch immer ein Fehler auftreten. Man sollte demnach versuchen, für jede approximierende Funktion die Größenordnung der Differenz, also des Fehlers zu bestimmen. Die folgenden Begriffe sind dazu sehr nützlich.

Es seien $f(x)$, $h(x)$ positive, reellwertige, stetige und für alle $x \geq x_0 > 0$ definierte Funktionen.

Die Schreibweise $f(x) \sim h(x)$ bedeutet, dass $\lim_{x\to\infty}(f(x)/h(x)) = 1$; $f(x)$ und $h(x)$ nennt man in diesem Fall *asymptotisch gleich*, wenn x gegen Unendlich geht. Man beachte, dass die Differenz der Funktionen durchaus ins Unendliche wachsen kann.

Wenn unter Annahme obiger Eigenschaften Konstanten C, C', $0 < C < C'$, und x_0, x_1 mit $x_1 \geq x_0$ derart existieren, dass $C \leq f(x)/h(x) \leq C'$ für alle $x \geq x_1$ gilt, dann sagt man, $f(x)$ und haben $h(x)$ *die gleiche Größenordnung.*

Es seien $f(x)$, $g(x)$, $h(x)$ reellwertige, stetige und für alle $x \geq x_0 > 0$ definierte Funktionen. Zudem gelte $h(x) > 0$ für alle $x \geq x_0$. Dann bedeutet die Schreibweise

$$f(x) = g(x) + O(h(x)),$$

dass die Differenz der Funktionen $f(x)$ und $g(x)$ letztendlich durch ein konstantes Vielfaches der Funktion $h(x)$ beschränkt ist (für x gegen Unendlich); das heißt, es existieren $C > 0$ und $x_1 \geq x_0$ derart, dass für jedes $x \geq x_1$ die Ungleichung $|f(x) - g(x)| \leq Ch(x)$ erfüllt ist. Diese nützliche Bezeichnungsweise wird dazu verwendet, den Fehler auszudrücken, den man begeht, wenn man $f(x)$ durch $g(x)$ ersetzt.

In ähnlicher Weise bezeichnet

$$f(x) = g(x) + o(h(x)),$$

dass $\lim_{x\to\infty}[f(x) - g(x)]/h(x) = 0$. Dies bedeutet intuitiv, dass der Fehler im Vergleich zu $h(x)$ vernachlässigbar ist.

A Historische Entwicklung

Es ist zweckmäßig, die verschiedenen Entdeckungen zur Verteilung der Primzahlen in ihrer geschichtlichen Reihenfolge bis hin zum Primzahlsatz vorzustellen. Diesen Weg beschritt Landau in seiner berühmten Abhandlung *Handbuch der Lehre von der Verteilung der Primzahlen*, der klassischen Arbeit zum Thema. Eine andere Darstellung von historischem Interesse und vor Landau ist in einem sehr langen Artikel von Torelli (1901) zu finden (in Italienisch verfasst).

Euler

Zunächst werde ich ein Resultat von Euler vorstellen, das nicht nur die Unendlichkeit der Anzahl der Primzahlen enthält, sondern zudem aussagt, dass „die Primzahlen nicht so dünn gesät sind wie die Quadratzahlen." (Diese Aussage wird gleich präzisiert.)

Euler zeigte, dass die Reihe $\sum_{n=1}^{\infty}(1/n^{\sigma})$ für jede reelle Zahl $\sigma > 1$ konvergent ist und sogar für jedes $\sigma_0 > 1$ auf der Halbgeraden $\sigma_0 \leq x < \infty$ gleichmäßig konvergiert. Daher definiert die Reihe eine stetige und differenzierbare Funktion $\zeta(\sigma)$ (für $1 < \sigma < \infty$). Darüber hinaus ist $\lim_{\sigma\to\infty}\zeta(\sigma) = 1$ und $\lim_{\sigma\to 1+0}(\sigma - 1)\zeta(\sigma) = 1$. Die Funktion $\zeta(\sigma)$ nennt man die *Zetafunktion*.

Das Verbindungsglied zwischen der Zetafunktion und den Primzahlen ist das folgende Eulersche Produkt, das die Eindeutigkeit der Zerlegung der ganzen Zahlen als Produkt von Primzahlen ausdrückt:

$$\sum_{n=1}^{\infty} \frac{1}{n^\sigma} = \prod_p \frac{1}{1 - \frac{1}{p^\sigma}} \quad \text{(für } \sigma > 1\text{)}.$$

Es folgt insbesondere, dass $\zeta(\sigma) \neq 0$ für $\sigma > 1$.

Mit derselben Idee, die er auch in seinem Beweis der Existenz unendlich vieler Primzahlen verwendet hatte (siehe Kapitel 1), bewies Euler im Jahre 1737:

Die Reihe der Inversen der Primzahlen ist divergent: $\sum_p (1/p) = \infty$.

Beweis. Es sei N eine beliebige natürliche Zahl. Jede ganze Zahl $n \leq N$ ist in eindeutiger Weise ein Produkt von Potenzen von Primzahlen p, $p \leq n \leq N$. Zudem gilt für jede Primzahl p,

$$\sum_{k=0}^{\infty} \frac{1}{p^k} = \frac{1}{1 - \frac{1}{p}}\,.$$

Daraus folgt

$$\sum_{n=1}^{N} \frac{1}{n} \leq \prod_{p \leq N} \left(\sum_{k=0}^{\infty} \frac{1}{p^k} \right) = \prod_{p \leq N} \frac{1}{1 - \frac{1}{p}}\,.$$

Da aber

$$\log \prod_{p \leq N} \frac{1}{1 - \frac{1}{p}} = - \sum_{p \leq N} \log \left(1 - \frac{1}{p} \right),$$

und für jede Primzahl p,

$$\begin{aligned} - \log \left(1 - \frac{1}{p} \right) &= \sum_{m=1}^{\infty} \frac{1}{mp^m} \leq \frac{1}{p} + \frac{1}{p^2} \left(\sum_{h=0}^{\infty} \frac{1}{p^h} \right) \\ &= \frac{1}{p} + \frac{1}{p^2} \times \frac{1}{1 - \frac{1}{p}} = \frac{1}{p} + \frac{1}{p(p-1)} \\ &< \frac{1}{p} + \frac{1}{(p-1)^2}\,. \end{aligned}$$

Somit ist

$$\log \sum_{n=1}^{N} \frac{1}{n} \leq \log \prod_{p \leq N} \frac{1}{1 - \frac{1}{p}} \leq \sum_{p \leq N} \frac{1}{p} + \sum_{p \leq N} \frac{1}{(p-1)^2}$$
$$\leq \sum_{p} \frac{1}{p} + \sum_{n=1}^{\infty} \frac{1}{n^2}\,.$$

Aber die Reihe $\sum_{n=1}^{\infty}(1/n^2)$ ist konvergent. Da N beliebig war und die harmonische Reihe divergiert, ist $\log \sum_{n=1}^{\infty}(1/n) = \infty$ und deshalb divergiert auch $\sum_p(1/p)$. □

Wie im Beweis erwähnt, ist die Reihe $\sum_{n=1}^{\infty}(1/n^2)$ konvergent. Daher könnte man etwas vage ausgedrückt sagen, dass die Primzahlen nicht so dünn gesät sind wie die Quadratzahlen.

Eine der wunderbaren Entdeckungen von Euler ist die Summe dieser Reihe:

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}\,.$$

Euler wertete auch die Summen $\sum_{n=1}^{\infty}(1/n^{2k})$ für jedes $k \geq 1$ aus, womit ein recht schwer greifbares Problem gelöst war. Dazu bediente er sich der Bernoulli-Zahlen, die wie folgt definiert sind:

$$B_0 = 1, \quad B_1 = -\frac{1}{2}\,, \quad B_2 = \frac{1}{6}\,, \ \ldots\ ,$$

B_k ist nun rekursiv durch die Relation

$$\binom{k+1}{1} B_k + \binom{k+1}{2} B_{k-1} + \cdots + \binom{k+1}{k} B_1 + B_0 = 0$$

gegeben. Diese Zahlen sind offensichtlich rational und man kann einfach zeigen, dass $B_{2k+1} = 0$ für jedes $k \geq 1$. Die Bernoulli-Zahlen tauchen auch als Koeffizienten in dieser Taylorreihenentwicklung auf:

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} x^k.$$

Unter Verwendung der Formel von Stirling,

$$n! \sim \frac{\sqrt{2\pi} n^{n+\frac{1}{2}}}{e^n} \qquad (\text{für } n \to \infty),$$

lässt sich zudem zeigen, dass

$$|B_{2n}| \sim 4\sqrt{\pi n}\left(\frac{n}{\pi e}\right)^{2n};$$

daher konvergiert obige Reihe im Intervall $|x| < 2\pi$.

Euler hatte die Bernoulli-Zahlen bereits früher verwendet, um Summen gleicher Potenzen aufeinander folgender Zahlen auszudrücken:

$$\sum_{j=1}^{n} j^k = S_k(n) \quad (k \geq 1),$$

wobei

$$S_k(X) = \frac{1}{k+1}\left[X^{k+1} - \binom{k+1}{1}B_1X^k + \binom{k+1}{2}B_2X^{k-1} + \cdots + \binom{k+1}{k}B_kX\right].$$

Zu einem ähnlichen Ausdruck gelangte etwa zur gleichen Zeit auch Seki in Japan.

Eulers Formel für den Wert von $\zeta(2k)$ ist:

$$\zeta(2k) = \sum_{n=1}^{\infty}\frac{1}{n^{2k}} = (-1)^{k+1}\frac{(2\pi)^{2k}B_{2k}}{2(2k)!}.$$

Insbesondere ist

$$\zeta(2) = \sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6} \quad \text{(bereits erwähnt)},$$

$$\zeta(4) = \sum_{n=1}^{\infty}\frac{1}{n^4} = \frac{\pi^4}{90}, \quad \text{usw.}$$

Euler betrachtete auch die durch

$$B_k(X) = \sum_{i=0}^{k}\binom{k}{i}B_iX^{k-i} \quad (k \geq 0)$$

definierten Bernoulli-Polynome, die man dazu verwenden könnte, den Ausdruck für $S_k(X)$ umzuschreiben. Wichtiger aber ist ihre Anwendung auf eine weitreichende Verallgemeinerung der Abelschen Summationsformel, nämlich der wohlbekannten Euler-MacLaurin-Summenformel:

Wenn $f(x)$ eine stetige, beliebig oft stetig differenzierbare Funktion ist und $a < b$ ganze Zahlen sind, dann gilt für jedes $k \geq 1$,

$$\sum_{n=a+1}^{b} f(n) = \int_a^b f(t)dt + \sum_{r=1}^{k}(-1)^r \frac{B_r}{r!}\left\{f^{(r-1)}(b) - f^{(r-1)}(a)\right\} + \frac{(-1)^{k-1}}{k!}\int_a^b B_k(t-[t])f^{(k)}(t)dt$$

(das Symbol $[t]$ bezeichnet wie zuvor den ganzzahligen Anteil von t).

Dem Leser sei dringend angeraten, den Artikel von Ayoub, *Euler and the zeta function* (1974), zu konsultieren. Darin befindet sich eine Beschreibung vieler einfallsreicher Entdeckungen von Euler bezüglich $\zeta(s)$ – einige vollständig begründet, einige nur unter Vorausahnung späterer Arbeiten von Riemann plausibel gemacht.

Legendre

Den ersten ernst zu nehmenden Versuch, die Funktion $\pi(x)$ zu studieren, unternahm Legendre (1808), der das Sieb des Eratosthenes verwendete, um zu zeigen, dass

$$\pi(N) = \pi(\sqrt{N}) - 1 + \sum \mu(d)\left[\frac{N}{d}\right].$$

Die Summation erstreckt sich über alle Teiler d des Produkts aller Primzahlen $p \leq \sqrt{N}$, $\mu(n)$ bezeichnet die bereits in Kapitel 3, Abschnitt I definierte Möbius-Funktion.

Als Konsequenz daraus schloss Legendre, dass $\lim_{x\to\infty}(\pi(x)/x) = 0$, was jedoch ein eher schwaches Resultat ist.

Aufgrund von Experimenten hatte Legendre bereits 1798 vermutet und 1808 erneut geäußert, dass

$$\pi(x) = \frac{x}{\log x - A(x)},$$

wobei $\lim_{x\to\infty} A(x) = 1{,}08366\ldots$. Vierzig Jahre später zeigte Tschebyscheff (siehe unten), dass wenn der Grenzwert $\lim_{x\to\infty} A(x)$ existiert, dieser gleich 1 sein muss. Einen einfacheren Beweis für diese Tatsache gab Pintz (1980) an.

Gauß

Im Alter von 15 Jahren vermutete Gauß 1792, dass $\pi(x)$ und der durch

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t},$$

definierte Integrallogarithmus asymptotisch gleich sind. Aus $\mathrm{Li}(x) \sim x/\log x$ folgt daher

$$\pi(x) \sim \frac{x}{\log x},$$

was implizit auch von Legendre vermutet worden war. Diese Vermutung wurde schließlich bestätigt und ist heute als *Primzahlsatz* bekannt; ich werde in Kürze darauf zurückkommen.

Die Approximation von $\pi(x)$ durch $x/\log x$ ist zwar einigermaßen gut, es ist jedoch besser, den Integrallogarithmus zu verwenden, was auch in Tabelle 14 ersichtlich wird.

Tschebyscheff

Ein entscheidender Fortschritt bei der Bestimmung der Größenordnung von $\pi(x)$ gelang Tschebyscheff um 1850. Er bewies mit elementaren Methoden, dass es für jedes $\varepsilon > 0$ ein $x_0 > 0$ derart gibt, dass für $x > x_0$,

$$(C' - \varepsilon)\frac{x}{\log x} < \pi(x) < (C + \varepsilon)\frac{x}{\log x},$$

wobei

$$C' = \log \frac{2^{1/2}\, 3^{1/3}\, 5^{1/5}}{30^{1/30}} = 0{,}92129\ldots, \quad C = \frac{6}{5}\, C' = 1{,}10555\ldots\ .$$

Darüber hinaus zeigte Tschebyscheff, dass wenn der Grenzwert von

$$\frac{\pi(x)}{x/\log x}$$

existiert (für $x \to \infty$), dieser gleich 1 sein muss. Er folgerte auch, dass Legendres Approximation von $\pi(x)$ nicht wahr sein kann, es sei denn, man ersetzt 1,08366 durch 1 (siehe Landaus Buch, Seite 17).

Tschebyscheff bewies zudem Bertrands Postulat über die Existenz mindestens einer Primzahl zwischen einer beliebigen natürlichen Zahl $n \geq 2$ und $2n$. Ich werde Bertrands Postulat während der Vorstellung der wesentlichen Eigenschaften von $\pi(x)$ noch detaillierter besprechen.

Tschebyscheff arbeitete mit der Funktion $\theta(x) = \sum_{p \leq x} \log p$, die man heute *Tschebyscheff-Funktion* nennt. Diese trägt im Prinzip dieselbe Information wie $\pi(x)$, ist aber in gewisser Weise einfacher zu handhaben.

Obwohl Tschebyscheff dem von Gauß vermuteten fundamentalen Primzahlsatz schon recht nahe kam, dauerte es noch etwa 50 Jahre,

bis der Beweis am Ende des Jahrhunderts schließlich gefunden war. Während dieser Zeit steuerte Riemann wichtige neue Ideen bei.

Riemann

Riemann kam auf die Idee, die Zetafunktion auf komplexe Zahlen s mit Realteil größer als 1 auszudehnen, nämlich

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}\,.$$

Das Euler-Produkt behält dabei für komplexes s mit $\mathrm{Re}(s) > 1$ nach wie vor seine Gültigkeit.

Unter Verwendung der Euler-MacLaurin-Summenformel lässt sich $\zeta(s)$ wie folgt ausdrücken:

$$\zeta(s) = \frac{1}{s-1} + \frac{1}{2} + \sum_{r=2}^{k} \frac{B_r}{r!} s(s+1)\cdots(s+r-2) \\ - \frac{1}{k!} s(s+1)\cdots(s+k-1) \int_1^{\infty} B_k(x-[x]) \frac{dx}{x^{s+k}}\,.$$

Dabei ist $k \geq 1$ eine beliebige natürliche Zahl, die Zahlen B_r sind die Bernoulli-Zahlen, die man nicht mit $B_k(x-[x])$, dem Wert des k-ten Bernoulli-Polynoms $B_k(X)$ an der Stelle $x-[x]$ verwechseln sollte.

Das Integral konvergiert für $\mathrm{Re}(s) > 1-k$, und da k eine beliebige natürliche Zahl ist, bedeutet die Formel die holomorphe Fortsetzung von $\zeta(s)$ auf die ganze Ebene. $\zeta(s)$ ist überall holomorph, mit Ausnahme des einfachen Pols $s = 1$ mit Residuum 1, das heißt,

$$\lim_{s\to 1}(s-1)\zeta(s) = 1.$$

Riemann führte 1859 die Funktionalgleichung für die Zetafunktion ein. Da die Funktionalgleichung die Gamma-Funktion $\Gamma(s)$ enthält, soll diese nun zunächst definiert werden, was für $\mathrm{Re}(s) > 0$ bequem anhand des Eulerschen Integrals erfolgen kann:

$$\Gamma(s) = \int_0^{\infty} e^{-u} u^{s-1} du.$$

Für beliebige komplexe Zahlen s kann man die Definition durch

$$\Gamma(s) = \frac{1}{s e^{\gamma s}} \prod_{n=1}^{\infty} \frac{e^{s/n}}{1+\frac{s}{n}}\,,$$

ersetzen, wobei γ die Eulersche Konstante ist:

$$\gamma = \lim_{n\to\infty} \left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n\right) = 0{,}577215665\ldots\ .$$

Eulers Konstante, von den Italienern mit gutem Grund auch Mascheronis Konstante genannt, ist durch die folgende Formel von Mertens mit dem Euler-Produkt verbunden:

$$e^{\gamma} = \lim_{n\to\infty} \frac{1}{\log p_n} \prod_{i=1}^{n} \frac{1}{1 - \dfrac{1}{p_i}}\,.$$

$\Gamma(s)$ nimmt niemals den Wert 0 an; die Funktion ist mit Ausnahme der einfachen Pole an den Stellen 0, -1, -2, $-3,\ldots$ überall holomorph. Für jede positive ganze Zahl n ist $\Gamma(n) = (n-1)!$, das heisst, die Gamma-Funktion stellt eine Erweiterung der Fakultätsfunktion dar. Sie erfüllt viele interessante Relationen, darunter zum Beispiel die Funktionalgleichungen

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}, \qquad \Gamma(s+1) = s\Gamma(s),$$

und

$$\Gamma(s)\Gamma\left(s + \frac{1}{2}\right) = \frac{\sqrt{\pi}}{2^{2s-1}}\Gamma(2s).$$

Hier nun die Funktionalgleichung für die Riemannsche Zetafunktion:

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s).$$

Aus der Funktionalgleichung folgt zum Beispiel, dass $\zeta(0) = -\frac{1}{2}$.

Die Nullstellen der Zetafunktion sind:

(a) Einfache Nullstellen an den Punkten -2, -4, $-6,\ldots$, die man triviale Nullstellen nennt.

(b) Nullstellen auf dem kritischen Streifen der nichtreellen komplexen Zahlen s mit $0 \le \mathrm{Re}(s) \le 1$.

In der Tat gilt nach Eulers Produkt $\zeta(s) \neq 0$, wenn $\mathrm{Re}(s) > 1$. Falls $\mathrm{Re}(s) < 0$, dann $\mathrm{Re}(1-s) > 1$ und die rechte Seite der Funktionalgleichung ist ungleich Null, so dass die Nullstellen genau $s = -2, -4, -6,\ldots$ sein müssen, und dies sind die Pole von $\Gamma(s/2)$.

Die Kenntnis der Nullstellen der Zetafunktion hat einen tiefgreifenden Einfluss auf das Verständnis der Verteilung der Primzahlen. Man kann zunächst feststellen, dass die Nullstellen im kritischen Streifen nicht reell sind und zudem symmetrisch zur reellen Achse und der vertikalen Geraden $\mathrm{Re}(x) = \frac{1}{2}$ liegen.

Riemann vermutete, dass alle nichttrivialen Nullstellen ρ von $\zeta(s)$ auf der kritischen Geraden $\mathrm{Re}(s) = \frac{1}{2}$ liegen, das heißt, $\rho = \frac{1}{2} + i\gamma$. Dies ist die berühmte, bis heute unbewiesene *Riemannsche Vermutung*. Es handelt sich hierbei zweifelsfrei um eines der schwierigsten und wichtigsten Probleme der Zahlentheorie und sicher auch der gesamten Mathematik. Ich werde in Kürze darauf zurückkommen und von einigen modernen Entwicklungen berichten.

An dieser Stelle soll kurz umrissen werden, wie Riemann zu einer genaueren Abschätzung für $\pi(x)$ gelangte. Er zählte auch Primzahlpotenzen p^n und gab ihnen ein Gewicht $1/n$. Das heißt, er definierte für jede reelle Zahl $x > 0$ den Ausdruck

$$J(x) = \pi(x) + \frac{1}{2}\,\pi(x^{1/2}) + \frac{1}{3}\,\pi(x^{1/3}) + \frac{1}{4}\,\pi(x^{1/4}) + \cdots\ .$$

Man beachte, dass die Summanden gleich 0 sind, sobald $2^n > x$, so dass obiger Ausdruck für jedes x eine endliche Summe ist. Unter Zuhilfenahme der Möbius-Funktion sowie der Möbiusschen Umkehrformel erhält man

$$\pi(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} J(x^{1/n})$$

(wiederum eine endliche Summe). Der wesentliche Teil der Arbeit war, eine analytische Formel für $J(x)$ in Form von Termen des Integrallogarithmus mit komplexen Argumenten zu finden.

Es sei $w = u + iv$ und z definiert als πi, $-\pi i$ oder 0, je nachdem, ob $v > 0$, $v < 0$ oder $v = 0$. Nach Definition,

$$\mathrm{Li}(e^w) = \int_C \frac{e^t}{t} dt,$$

wobei C die horizontale Linie $C = \{s + iv \mid -\infty < s \leq u\}$ ist. Riemann gelang es, die folgende fundamentale analytische Formel für die Funktion $J(x)$ zu beweisen: Für alle $x > 0$,

$$J(x) = \mathrm{Li}(x) - \sum_{\rho} \mathrm{Li}(x^{\rho}) - \log 2 + \int_x^{\infty} \frac{dt}{t(t^2-1)\log t}\,;$$

wobei die Summe über alle nichttrivialen Nullstellen ρ der Zetafunktion in der oberen Halbebene läuft. Einsetzen von $J(x^{1/n})$ in die Formel für $\pi(x)$ führt zum folgenden Ausdruck für $\pi(x)$, aufgebaut aus Termen des Integrallogarithmus:

$$\pi(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \mathrm{Li}(x^{1/n}) + \text{Terme, die die Nullstellen beinhalten.}$$

Sicher stellte die Rechtfertigung der heiklen analytischen Schritte hin zu dieser Darstellung selbst für Riemann eine Herausforderung dar; zudem ist die Abschätzung der Terme, die von den Nullstellen ρ abhängen, sehr schwierig. Ungeachtet dessen liefert die *Riemann-Funktion*

$$R(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \mathrm{Li}(x^{1/n})$$

eine exzellente Abschätzung für $\pi(x)$, wie durch Berechnungen bestätigt wurde (siehe auch Tabelle 14).

Die Riemann-Funktion lässt sich mit Hilfe der schnell konvergierenden Potenzreihe von Gram (1893) berechnen:

$$R(x) = 1 + \sum_{n=1}^{\infty} \frac{1}{n\zeta(n+1)} \times \frac{(\log x)^n}{n!}\,.$$

Die Arbeit von Riemann zur Primzahlverteilung wird in dem uneingeschränkt zu empfehlenden Buch von Edwards (1974) gründlich behandelt. Weitere Bücher über die Riemannsche Zetafunktion sind die klassische Abhandlung von Titchmarsh (1951), sowie die neueren Bände von Ivić (1985) und Patterson (1988).

de la Vallée Poussin und Hadamard

Riemann stellte viele der Werkzeuge für den Beweis des fundamentalen *Primzahlsatzes*

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

zur Verfügung. Andere Werkzeuge kamen aus der komplexen Funktionentheorie, die sich damals in einer Blütezeit befand.

Der Beweis des Primzahlsatzes wurde zum „meistgesuchten“ Beweis erkoren und man behauptete, dass der, der ihn findet, unsterblich werden würde.

Der Satz wurde schließlich nicht von einem, sondern von zwei hervorragenden Analytikern bewiesen, und zwar unabhängig voneinander

im selben Jahr (1896). Nein, sie wurden zwar nicht unsterblich, wie dies in einigen griechischen Legenden der Fall ist. Aber fast! Hadamard wurde 98 Jahre alt, de la Vallée Poussin lebte fast so lang, er wurde 96.

De la Vallée Poussin kam zu folgendem Ergebnis: Es gibt $c > 0$ und $t_0 = t_0(c) > e^{2c}$ derart, dass $\zeta(s) \neq 0$ für jedes $s = \sigma + it$ im Bereich:

$$\begin{cases} 1 - \dfrac{c}{\log t_0} \leq \sigma \leq 1, & \text{wenn } |t| \leq t_0, \\ 1 - \dfrac{c}{\log |t|} \leq \sigma \leq 1, & \text{wenn } t_0 \leq |t|. \end{cases}$$

Insbesondere ist $\zeta(1 + it) \neq 0$ für jedes t, wie von Hadamard gezeigt.

Die Bestimmung eines großen, nullstellenfreien Bereichs für $\zeta(s)$ war von entscheidender Bedeutung beim Beweis des Primzahlsatzes.

Hadamard und de la Vallée Poussin bewiesen jedoch nicht nur den Primzahlsatz, sondern gaben auch eine Abschätzung für den Fehlerterm an:

$$\pi(x) = \mathrm{Li}(x) + O\big(xe^{-A\sqrt{\log x}}\big),$$

mit einer positiven Konstanten A. Ich werde bald berichten, wie man durch Erweiterung des nullstellenfreien Bereichs der Zetafunktion zu einer besseren Abschätzung des Fehlerterms gelangen kann.

Es gibt inzwischen viele Varianten des Beweises, die auf analytischen Methoden beruhen. Sie sind in verschiedenen Artikeln und Büchern beschrieben; siehe zum Beispiel Grosswald (1964). Ein besonders einfacher Beweis stammt von Newman (1980).

Man kann den Primzahlsatz in anderer Form äquivalent ausdrücken. Unter Verwendung der Tschebyscheff-Funktion lautet der Satz so:

$$\theta(x) \sim x.$$

Eine weitere Formulierung beinhaltet die summatorische Funktion der *von Mangoldt-Funktion*. Es sei

$$\Lambda(n) = \begin{cases} \log p & \text{wenn } n = p^\nu \ (\nu \geq 1) \text{ und } p \text{ eine Primzahl ist,} \\ 0 & \text{sonst.} \end{cases}$$

Diese durch von Mangoldt eingeführte Funktion hat die folgende interessante Eigenschaft im Zusammenhang mit der logarithmischen Ableitung der Zetafunktion:

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}, \qquad \text{für } \mathrm{Re}(s) > 1.$$

Sie steht auch in Verbindung mit der Funktion $J(x)$, die schon einmal in Erscheinung getreten war:

$$J(x) = \sum_{n \le x} \frac{\Lambda(n)}{\log n}\,.$$

Die summatorische Funktion von $\Lambda(n)$ ist definiert als

$$\psi(x) = \sum_{n \le x} \Lambda(n).$$

Diese lässt sich leicht in Form von Termen der Tschebyscheff-Funktion ausdrücken:

$$\psi(x) = \theta(x) + \theta(x^{1/2}) + \theta(x^{1/3}) + \cdots\,.$$

Der Primzahlsatz lässt sich auch so formulieren:

$$\psi(x) \sim x.$$

Erdös und Selberg

Man glaubte eine lange Zeit, dass sich die Verwendung analytischer Methoden beim Beweis des Primzahlsatzes nicht vermeiden ließe. Umso erstaunter war die mathematische Welt, als sowohl Erdös als auch Selberg 1949 zeigten, wie man den Primzahlsatz mit ausschließlich elementaren Abschätzungen von arithmetischen Funktionen beweisen kann.

Viele solcher Abschätzungen waren bereits bekannt gewesen, so zum Beispiel

$$\sum_{n \le x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right), \quad \text{wobei } \gamma \text{ die Euler-Konstante ist,}$$

$$\sum_{n \le x} \frac{1}{n^\sigma} = \frac{x^{1-\sigma}}{1-\sigma} + \zeta(\sigma) + O\left(\frac{1}{x^\sigma}\right), \quad \text{wobei } \sigma > 1,$$

$$\sum_{n \le x} \log n = x \log x - x + O(\log x),$$

$$\sum_{n \le x} \frac{\log n}{n} = \frac{1}{2}(\log x)^2 + C + O\left(\frac{\log x}{x}\right).$$

Obige Abschätzungen kann man mit Hilfe der Summationsformeln von Abel oder Euler-MacLaurin gewinnen, sie haben an sich keine

arithmetische Bedeutung. Die folgenden Summen, die Primzahlen enthalten, sind schon interessanter:

$$\sum_{p\le x}\frac{\log p}{p} = \log x + O(1),$$
$$\sum_{p\le x}\frac{1}{p} = \log\log x + C + O\left(\frac{1}{\log x}\right), \quad \text{mit } C = 0{,}2615\ldots,$$
$$\sum_{n\le x}\frac{\Lambda(n)}{n} = \log x + O(1),$$
$$\sum_{n\le x}\frac{\Lambda(n)\log n}{n} = \frac{1}{2}(\log x)^2 + O(\log x).$$

Selberg gelangte 1949 zu folgender Abschätzung:

$$\sum_{p\le x}(\log p)^2 + \sum_{pq\le x}(\log p)(\log q) = 2x\log x + O(x),$$

wobei p, q Primzahlen sind.

Diese Abschätzung ist jeweils äquivalent zu den folgenden:

$$\theta(x)\log x + \sum_{p\le x}\theta\left(\frac{x}{p}\right)\log p = 2x\log x + O(x),$$
$$\sum_{n\le x}\Lambda(n)\log n + \sum_{mn\le x}\Lambda(m)\Lambda(n) = 2x\log x + O(x).$$

Aufgrund seiner Abschätzung war Selberg in der Lage, einen elementaren Beweis des Primzahlsatzes anzugeben. Zur gleichen Zeit fand Erdös, ebenfalls unter Verwendung einer Variante von Selbergs Abschätzung

$$\frac{\psi(x)}{x} + \frac{1}{\log x}\sum_{n\le x}\frac{\psi(x/n)}{x/n}\,\frac{\Lambda(n)}{n} = 2 + O\left(\frac{1}{\log x}\right),$$

mit Hilfe einer anderen elementaren Methode seinen Beweis des Primzahlsatzes.

Diamond & Steinig fanden 1970 einen elementaren Beweis, der zudem einen expliziten Fehlerterm enthält. Diamond (1982) veröffentlichte einen maßgeblichen, detaillierten Artikel über elementare Methoden bei der Verteilung von Primzahlen.

B Summen unter Einschluss der Möbius-Funktion

Schon bevor Möbius die Funktion $\mu(n)$ formal definiert hatte, war sie von Euler untersucht worden. Er vermutete 1748 auf Grundlage experimenteller Berechnungen, dass $\sum_{n=1}^{\infty} \mu(n)/n$ gegen 0 konvergiert. Von Mangoldt bewies diese Vermutung als Anwendung des Primzahlsatzes. Tatsächlich gilt sogar die Umkehrung: Die Konvergenz der Reihe gegen 0 impliziert den Primzahlsatz.

Des Weiteren gilt für jedes s mit $\mathrm{Re}(s) > 1$,

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}\,.$$

Insbesondere folgt mit $s = 2$ für jedes $x > 1$,

$$\sum_{n \le x} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2} + O\left(\frac{1}{x}\right).$$

Die summatorische Funktion der Möbius-Funktion ist die *Mertens-Funktion*

$$M(x) = \sum_{n \le x} \mu(n).$$

Man kann zeigen, dass der Primzahlsatz auch gleichbedeutend damit ist, dass $\lim_{x\to\infty} M(x)/x = 0$. Details zu den vorangegangenen Aussagen finden sich in den Büchern von Landau (1909), Ayoub (1963) oder Apostol (1976).

Daboussi fand 1984 einen elementaren Beweis für $\lim_{x\to\infty} M(x)/x = 0$ und damit auch einen weiteren elementaren Beweis des Primzahlsatzes, ohne auf Selbergs Ungleichung zurückgreifen zu müssen.

Was die Größenordnung von $M(x)$ angeht, so vermutete Mertens selbst, dass $|M(x)| < \sqrt{x}$. Klassische Zahlentheoretiker wie Stieltjes und Hadamard waren an der Untersuchung dieses wichtigen und schwierigen Problems beteiligt. Schließlich gelang es Odlyzko & te Riele 1985, die Vermutung zu widerlegen. Sie zeigten, dass

$$\limsup_{x\to\infty} \frac{M(x)}{\sqrt{x}} > 1{,}06, \qquad \liminf_{x\to\infty} \frac{M(x)}{\sqrt{x}} < -1{,}009\,.$$

In einem 1987 erschienenen Artikel von Pintz befindet sich ein Beweis, in dem ein effektives x_0 mit $\log x_0 < 3{,}21 \times 10^4$ angegeben ist, für das die Mertenssche Vermutung falsch wird. Details dazu finden sich im Artikel von te Riele (1985).

C Primzahltabellen

Ich werde mein Augenmerk nun auf Primzahltabellen sowie Tabellen von Faktoren von Zahlen richten, die nicht durch 2, 3 oder 5 teilbar sind. Die ersten umfangreicheren Tabellen stammen von Brancker 1668 (Tabelle der kleinsten Faktoren der Zahlen bis 100 000), Krüger 1746 (Primzahlen bis 100 000), Lambert 1770 (Tabelle der kleinsten Faktoren der Zahlen bis 102 000), Felkel 1776 (Tabelle der kleinsten Faktoren der Zahlen bis 408 000), Vega 1797 (Primzahlen bis 400 031), Chernac 1811 (Primfaktoren von Zahlen bis 1 020 000) und Burckhardt 1816/7 (kleinste Faktoren der Zahlen bis 3 036 000).

Sowohl Legendre als auch Gauß begründeten ihre empirischen Beobachtungen auf den jeweils vorhandenen Tabellen.

Nach und nach wurden die Tabellen erweitert. Im Jahre 1856 legte Crelle der Berliner Akademie eine Tabelle aller Primzahlen bis 6 000 000 vor. Diese Arbeit wurde vor 1861 von Dase auf alle Primzahlen bis 9 000 000 ausgedehnt.

Die erstaunlichste Leistung in diesem Zusammenhang erbrachte Kulik, der eine Tabelle der Faktoren aller Zahlen bis 100 330 220 anfertigte (außer den Vielfachen von 2, 3, 5), erschienen unter dem Titel *Magnus Canon Divisorum pro omnibus numeris per* 2, 3 *et* 5 *non divisibilibus, et numerorum primorum interfacentium ad millies centena millia accuratius ad* 100 300 201 *usque*. Kulik verbrachte etwa 20 Jahre mit der Erstellung dieser Tabelle. Nach seinem Tod im Jahre 1863 wurde das 8-bändige Werk mit insgesamt 4212 Seiten bei der Akademie der Wissenschaften in Wien hinterlegt (im Februar 1867).

Im Jahre 1909 veröffentlichte D. N. Lehmer eine Tabelle der Faktoren aller Zahlen bis etwa 10 000 000, eine Liste aller Primzahlen bis zu dieser Grenze folgte 1914. In diesem Fall fanden die Bände weite Verbreitung und waren den Mathematikern somit leicht zugänglich.

Mit dem Aufkommen von Computern wurden viele Tabellen auf Magnetband verfügbar. Sie lassen sich zudem mit Hilfe des Siebs des Eratosthenes in jedem Intervall vernünftiger Größe einfach erstellen.

Den treuen Lesern, die bis zu dieser Stelle gekommen sind, habe ich diesem Buch als Zeichen der Anerkennung und zu ihrer größten Annehmlichkeit eine Tabelle aller Primzahlen bis 10000 angefügt, sie folgt direkt auf das Literaturverzeichnis. Amüsieren Sie sich gut!

D Exakte Werte von $\pi(x)$ und Vergleiche mit $x/\log x$, $\mathrm{Li}(x)$ und $R(x)$

Berechnung des genauen Wertes von $\pi(x)$

Genaue Werte von $\pi(x)$ lassen sich durch direktes Zählen in Tabellen gewinnen. Oder aber durch eine geniale Methode, die sich Meissel 1871 ausdachte und die es ihm erlaubte, weit über den Umfang verfügbarer Tabellen hinaus zu gehen. Um $\pi(x)$ zu berechnen, setzt die Methode die Kenntnis der Primzahlen $p \le x^{1/2}$ sowie von Werten $\pi(y)$ für $y \le x^{2/3}$ voraus. Sie beruht auf der Formel

$$\pi(x) = \varphi(x,m) + m(s+1) + \frac{s(s-1)}{2} - 1 - \sum_{i=1}^{s} \pi\left(\frac{x}{p_{m+i}}\right),$$

wobei $m = \pi(x^{1/3})$, $n = \pi(x^{1/2})$, $s = n - m$ und $\varphi(x,m)$ die Anzahl derjenigen Zahlen $a \le x$ angibt, die nicht durch $2, 3, \ldots, p_m$ teilbar sind.

Auch wenn die Berechnung von $\varphi(x,m)$ für großes m lange dauert, ist sie doch nicht besonders schwierig. Die Berechnung basiert auf den folgenden einfachen Tatsachen:

Rekursionsrelation.

$$\varphi(x,m) = \varphi(x,m-1) - \varphi\left(\left[\frac{x}{p_m}\right], m-1\right).$$

Divisionseigenschaft. Wenn $P_m = p_1 p_2 \cdots p_m$ sowie $0 \le r < P_m$ und $a \ge 0$, dann

$$\varphi(aP_m + r, m) = a\varphi(P_m) + \varphi(r,m).$$

Symmetrieeigenschaft. Wenn $\frac{1}{2}P_m < r < P_m$, dann

$$\varphi(r,m) = \varphi(P_m) - \varphi(P_m - r - 1, m).$$

Meissel bestimmte 1885 die Zahl $\pi(10^9)$ (fand jedoch einen Wert, der um 56 zu klein war). Einen einfachen Beweis von Meissels Formel gab Brauer 1946 an. Lehmer verbesserte und erweiterte 1959 die Methode von Meissel. Lagarias, Miller & Odlyzko gelang im Jahre 1985 durch den Einbau neuer Siebmethoden eine weitere Verbesserung.

Zunehmend große Werte von $\pi(x)$ wurden in den nachfolgend genannten Jahren bekannt gegeben:

1985: $\pi(4 \times 10^{16})$ von Lagarias, Miller & Odlyzko,

1994: $\pi(10^{18})$ von Deléglise und Rivat (veröffentlicht 1996),

1996: $\pi(10^{20})$ von Deléglise,

2000: $\pi(10^{21})$ von Gourdon,

2001: $\pi(4 \times 10^{22})$ von Gourdon und Demichel.

Die folgende Tabelle zeigt neben den Werten von $\pi(x)$ auch die Vergleichswerte $x/\log x$, $\mathrm{Li}(x)$ und $R(x)$.

Tabelle 14.
Werte von $\pi(x)$ und ein Vergleich mit $x/\log x$, $\mathrm{Li}(x)$ und $R(x)$

x	$\pi(x)$	$(x/\log x) - \pi(x)$	$\mathrm{Li}(x) - \pi(x)$	$R(x) - \pi(x)$
10^8	5 761 455	−332 774	754	97
10^9	50 847 534	−2 592 592	1 701	−79
10^{10}	455 052 511	−20 758 030	3 104	−1 828
10^{11}	4 118 054 813	−169 923 160	11 588	−2 318
10^{12}	37 607 912 018	−1 416 705 193	38 263	−1 476
10^{13}	346 065 536 839	−11 992 858 452	108 971	−5 773
10^{14}	3 204 941 750 802	−102 838 308 636	314 890	−19 200
10^{15}	29 844 570 422 669	−891 604 962 453	1 052 619	73 218
10^{16}	279 238 341 033 925	−7 804 289 844 393	3 214 632	327 052
10^{17}	2 623 557 157 654 233	−68 883 734 693 929	7 956 589	−598 255
10^{18}	24 739 954 287 740 860	−612 483 070 893 537	21 949 555	−3 501 366
10^{19}	234 057 667 276 344 607	−5 481 624 169 369 961	99 877 775	23 884 333
10^{20}	2 220 819 602 560 918 840	−49 347 193 044 659 702	222 744 643	−4 891 825
10^{21}	21 127 269 486 018 731 928	−446 579 871 578 168 707	597 394 254	−86 432 204
10^{22}	201 467 286 689 315 906 290	−4 060 704 006 019 620 994	1 932 355 208	−127 132 665

Rekord

Der größte bisher berechnete Wert von $\pi(x)$ wurde von T. Oliveira e Silva im Dezember 2008 bestimmt und beträgt

$$\pi(10^{23}) = 1\,925\,320\,391\,606\,803\,968\,923.$$

Dabei wurden auch die Zwischenwerte $\pi(h \times 10^{22})$ für $h = 1, 2, \ldots, 9$ festgehalten, die für $h = 1, 2, 4$ eine genaue Übereinstimmung mit früher ermittelten Werten zeigten.

Man hat übrigens auch errechnet, für welche Argumente x die Funktion $\pi(x)$ den runden Wert einer Zehnerpotenz annimmt. Der zur Zeit höchste Wert dieser Art ist

$$\pi(465\,675\,465\,116\,607\,065\,549) = 10^{19}.$$

Vergleich von $\pi(x)$ mit $x/\log x$

Bereits an früherer Stelle hatte ich Tschebyscheffs Ungleichungen für $\pi(x)$ erwähnt, die er vor der Zeit des Primzahlsatzes mit elementaren Methoden gewonnen hatte. Sylvester entwickelte 1892 Tschebyscheffs Methode weiter und gelangte zu den Abschätzungen

$$0{,}95695\,\frac{x}{\log x} < \pi(x) < 1{,}04423\,\frac{x}{\log x}$$

für jedes hinreichend große x (siehe auch Langevin, 1977).

Erdös gab einen eleganten, für Unterrichtszwecke geeigneten Beweis der schwächeren Ungleichungen

$$(\log 2 - \varepsilon)\,\frac{x}{\log x} < \pi(x) < (\log 4 + \varepsilon)\,\frac{x}{\log x}\,,$$

die für jedes $\varepsilon > 0$ und alle hinreichend großen x gelten.

Mit Hilfe einer sehr genauen Analyse fanden Rosser & Schoenfeld 1962 die Abschätzungen

$$\frac{x}{\log x}\left(1 + \frac{1}{2\log x}\right) < \pi(x) \quad \text{für} \quad x \geq 59$$

und

$$\pi(x) < \frac{x}{\log x}\left(1 + \frac{3}{2\log x}\right) \quad \text{für} \quad x > 1.$$

In seiner Dissertation verfeinerte Dusart (1998) diese und weitere Ergebnisse aus der Literatur und zeigte

$$\frac{x}{\log x}\left(1 + \frac{1}{\log x}\right) \leq \pi(x)$$

für $x \geq 599$, sowie

$$\pi(x) \leq \frac{x}{\log x}\left(1 + \frac{1{,}2762}{\log x}\right)$$

für $x > 1$. Bemerkenswert auch die von Dusart ermittelten Ungleichungen

$$\pi(x) < \frac{x}{\log x - 1{,}1} \quad \text{für} \quad x > 60184,$$

$$\pi(x) > \frac{x}{\log x - 1} \quad \text{für} \quad x > 5393.$$

Aus den Resultaten von Rosser & Schoenfeld (1962) folgt, dass $\pi(x) \geq x/\log x$, sobald $x \geq 11$.

Vergleich von $\pi(x)$ mit $\mathrm{Li}(x)$

Wie Gauß 1849 an J.F. Encke schrieb, hatte er bereits „seit vielen Jahren“ alle Primzahlen bis 3×10^6 „abgezählt und mit dem Integralwerth verglichen“ und dabei festgestellt, dass $\pi(x)$ für alle x unterhalb dieser Grenze kleiner als $\mathrm{Li}(x)$ bleibt. Seitdem wurde vermutet, dass dies für alle x gilt – bis Littlewood 1914 bewies, dass die Differenz $\mathrm{Li}(x)-\pi(x)$ unendlich oft das Vorzeichen wechselt!

Unter der Annahme der Riemannschen Vermutung (siehe den folgenden Teil E) zeigte Skewes 1933, dass der erste Vorzeichenwechsel für ein $x < 10^{10^{10^{34}}}$ auftreten muss. Diese Zahl war lange Zeit dafür berühmt, die größte zu sein, die in der Mathematik auf eine einigermaßen natürliche Weise auftaucht. Mit Hilfe einer anderen Methode, die bestimmte Kenntnisse über die nichttrivialen Nullstellen der Riemannschen Zetafunktion voraussetzt, konnte Lehman (1966) zeigen, dass es zwischen $1{,}53\times10^{1165}$ und $1{,}65\times10^{1165}$ mindestens 10^{500} Zahlen x gibt, für die $\pi(x) > \mathrm{Li(x)}$ gilt. Man kennt heute, sogar ohne die Riemannsche Vermutung vorauszusetzen, wesentlich kleinere Schranken für den ersten Vorzeichenwechsel der Differenz $\mathrm{Li}(x)-\pi(x)$. In einer erstmals 1986 erwähnten Berechnung (veröffentlicht 1987) zeigte te Riele, dass es schon zwischen $6{,}62\times10^{370}$ und $6{,}69\times10^{370}$ mehr als 10^{180} aufeinander folgende Zahlen x mit $\pi(x) > \mathrm{Li}(x)$ gibt.

Rekord

Im Jahre 2000 zeigten Bays & Hudson, dass es in der Nähe von $1{,}39822\times10^{316}$ mindestens 10^{153} Zahlen x gibt, für die $\pi(x)$ größer als $\mathrm{Li}(x)$ ist. Der Beweis erforderte die Kenntnis, mit einer gewissen Genauigkeit, der ersten 10^6 nichttrivialen Nullstellen der Riemannschen Zetafunktion sowie die Gewissheit, dass sämtliche Nullstellen $\sigma+it$ mit $t<10^7$ auf der kritischen Geraden liegen. Dies war durch Berechnungen von A. Odlyzko und anderen sichergestellt.

E Die nichttrivialen Nullstellen von $\zeta(s)$

Zur Erinnerung: Die Nullstellen der Riemannschen Zetafunktion sind die trivialen Nullstellen -2, -4, $-6,\ldots$, sowie die nichttrivialen Nullstellen $\sigma+it$, mit $0\le\sigma\le1$, das heißt, Nullstellen auf dem kritischen Streifen.

Zunächst werde ich die Nullstellen im ganzen kritischen Streifen betrachten, danach die auf der kritischen Geraden $\mathrm{Re}(s)=\frac{1}{2}$.

Da $\zeta(\overline{s}) = \zeta(s)$ (wobei der Balken die komplex konjugierte Zahl bedeutet), liegen die Nullstellen symmetrisch zur reellen Achse; es reicht also, die Nullstellen in der oberen Hälfte des kritischen Streifens zu betrachten.

Für jedes $t > 0$ kann die Zetafunktion nur endlich viele Nullstellen (oder gar keine) der Form $\sigma + it$ annehmen (für eine reelle Zahl σ). Daher ist es möglich, die nichttrivialen Nullstellen der Zetafunktion aufzuzählen: $\rho_n = \sigma_n + it_n$, mit $0 < t_1 \le t_2 \le t_3 \le \dots$.

Für jedes $T > 0$ bezeichne $N(T)$ die Anzahl der Nullstellen $\rho_n = \sigma_n + it_n$ auf dem kritischen Streifen, mit $0 < t_n \le T$. Ebenso sei $N_0(T)$ die Anzahl der Nullstellen $\frac{1}{2} + it$ der Riemannschen Zetafunktion, die auf der kritischen Geraden liegen, wobei $0 < t \le T$.

Natürlich ist $N_0(T) \le N(T)$ und Riemanns Vermutung ist gleichbedeutend damit, dass $N_0(T) = N(T)$ für jedes $T > 0$.

Hier die wichtigsten Resultate über $N(T)$. Zunächst vermutete Riemann, später durch von Mangoldt bewiesen:

$$N(T) = \frac{T}{2\pi}\left\{\log\left(\frac{T}{2\pi}\right) - 1\right\} + O(\log T).$$

Es folgt, dass es unendlich viele Nullstellen auf dem kritischen Streifen gibt.

Alle bekannten nichttrivialen Nullstellen von $\zeta(s)$ sind einfach und liegen auf der kritischen Geraden. Montgomery zeigte 1973 unter Annahme der Riemannschen Vermutung, dass mindestens zwei Drittel der nichttrivialen Nullstellen einfach sind.

Levinson bewies 1974, dass mindestens ein Drittel der nichttrivialen Nullstellen von Riemanns Zetafunktion auf der kritischen Geraden liegen. Genauer gilt für genügend großes T, $L = \log(T/2\pi)$ und $U = T/L^{10}$, dass

$$N_0(T+U) - N_0(T) > \frac{1}{3}\big(N(T+U) - N(T)\big).$$

Conrey verbesserte dieses Resultat 1989 und konnte $\frac{1}{3}$ durch $\frac{2}{5}$ ersetzen.

Inzwischen wurden umfangreiche Berechnungen der Nullstellen von $\zeta(s)$ durchgeführt. Zunächst berechnete Gram 1903 die ersten 15 Nullstellen (das heißt, ρ_n für $1 \le n \le 15$). Titchmarsh fand 1935 die Nullstellen ρ_n für $n \le 1041$. Zu Beginn des Computerzeitalters erreichte Lehmer $n = 35\,337$. Bis 1969 hatten Rosser, Yohe & Schoenfeld die ersten $3\,500\,000$ Nullstellen berechnet.

Nur damit sie diesem Buch nicht in schändlicher Weise fern bleibt, hier eine Tabelle der kleinsten Nullstellen $\rho_n = \frac{1}{2} + it_n$, $t_n > 0$:

Tabelle 15. Nichttriviale Nullstellen der Riemannschen Zetafunktion

n	t_n	n	t_n	n	t_n
1	14,134725	11	52,970321	21	79,337375
2	21,022040	12	56,446248	22	82,910381
3	25,010858	13	59,347044	23	84,735493
4	30,424876	14	60,831779	24	87,425275
5	32,935062	15	65,112544	25	88,809111
6	37,586178	16	67,079811	26	92,491899
7	40,918719	17	69,546402	27	94,651344
8	43,327073	18	72,067158	28	95,870634
9	48,005151	19	75,704691	29	98,831194
10	49,773832	20	77,144840	30	101,317851

In Edwards' Buch (1974) findet sich eine detaillierte Erklärung der Methode von Gram, Backlund, Hutchinson und Haselgrove zu deren Berechnung der kleinsten 300 Nullstellen von $\zeta(s)$. Wagon fasste 1986 die wesentlichen Informationen in einem kurzen Bericht zusammen.

Mit der Arbeit von Brent begann 1977 eine erhebliche Ausdehnung der Berechnungen, siehe Brent (1979). Das zuletzt veröffentlichte Resultat stammt von van de Lune, te Riele & Winter (1986), die feststellten, dass die ersten 1 500 000 001 nichttrivialen Nullstellen von $\zeta(s)$ sämtlich einfach sind, auf der kritischen Geraden liegen und einen Imaginärteil $0 < t < 545\,439\,823{,}215$ haben. Dieses Resultat erforderte über 1000 Stunden Rechenzeit auf einem der schnellsten Computer, die zu dieser Zeit existierten.

Rekord

X. Gourdon und P. Demichel berechneten 2004 die ersten 10 Billionen nichttrivialen Nullstellen der Riemannschen Zetafunktion, ohne dabei ein Gegenbeispiel zur Riemannschen Vermutung zu entdecken. Der betreffende Imaginärteil t erstreckte sich dabei bis etwa $2{,}446 \times 10^{12}$. Zuvor hatte S. Wedeniwski zusammen mit einem großen Team von Helfern die ersten 100 Milliarden nichttrivialen Nullstellen von $\zeta(s)$ berechnet und dabei Riemanns Vermutung für alle t mit $0 < t < 29\,538\,618\,432{,}236$ verifiziert.

Im Jahre 1988 fanden Odlyzko & Schönhage eine schnelle Methode zur simultanen Berechnung einer großen Anzahl von Nullstellen der

Zetafunktion. Diese Methode wurde dazu verwendet, 10 Milliarden Nullstellen nahe der 10^{22}-sten Nullstelle zu bestimmen. Nach Angaben Odlyzkos (2001) liegen alle auf der kritischen Geraden und geben außerdem Anlass zu weiteren Vermutungen bezüglich einer Verbindung mit Eigenwerten von Zufallsmatrizen. Odlyzko zufolge gibt es heuristische Gründe dafür, dass jedes Gegenbeispiel zur Riemannschen Vermutung (falls überhaupt existent) sehr weit von den Bereichen entfernt ist, die mit heutigen Algorithmen erreichbar sind.

Man mag sich fragen, warum es so wichtig wäre zu wissen, dass sich alle Nullstellen von $\zeta(s)$ auf der kritischen Geraden befinden. Tatsache ist, dass bisher alle Versuche von Mathematikern fehlschlugen, die Riemannsche Vermutung direkt zu beweisen. Der natürliche Weg ist daher, ihre Richtigkeit anzunehmen und Konsequenzen daraus abzuleiten. Falls sich eine solche Konsequenz als falsch herausstellen sollte, so würde folgen, dass die Vermutung Riemanns falsch ist (vorausgesetzt, das Korollar wurde korrekt abgeleitet).

Aber es ist genau das Gegenteil, was die Sache so spannend macht. Lang ersehnte, fantastische Resultate würden aus der Richtigkeit der Riemannschen Vermutung folgen. Natürlich ist nicht auszuschließen, dass diese Aussagen auch ohne Rückgriff auf Riemanns Vermutung bewiesen werden. Es soll nicht unerwähnt bleiben, dass viele der Spezialisten auf diesem Gebiet fest an die Riemannsche Vermutung glauben.

Das Ableiten von Konsequenzen aus Riemanns Vermutung (nachdem wir nun so damit vertraut sind, können wir wie alle schreiben: die RH[1]) wurde auf weitere wichtige Bereiche der Arithmetik und auch der Geometrie ausgedehnt. Es wurden verschiedene Arten einer erweiterten Riemannschen Vermutung (ERH[2]) eingeführt, die sich auf Verallgemeinerungen der Zetafunktion beziehen, zumeist auf die sogenannten *Dirichletschen L-Funktionen*.

Ein Beweisansatz für die RH geht auf Hilbert zurück, nämlich in einem geeigneten Hilbert-Raum einen Operator zu finden, dessen Eigenwerte mit den nichttrivialen Nullstellen der Zetafunktion zusammenfallen, und dann aufgrund von noch zu findenden Symmetrien abzuleiten, dass die Eigenwerte auf der kritischen Geraden liegen. Die große Schwierigkeit liegt darin, den richtigen Raum, Operator und die Symmetrie zu finden und schließlich die analytischen Fakten in das Bild einzufügen. In diesem Zusammenhang sei auf die Arbeit von Connes (1996) hingewiesen.

---

[1] *Riemann's Hypothesis*
[2] *Extended Riemann Hypothesis*

Auf der anderen Seite ergibt sich keine stichhaltige Begründung für die Richtigkeit der RH, wenn man nur (oder sogar) weiß, dass sich alle bisher berechneten Hunderte von Milliarden Nullstellen der Zetafunktion auf der kritischen Geraden befinden. Abweichungen könnten sich für viel größere Nullstellen ergeben; ein von einer log log log-Funktion beherrschtes Verhalten oder Phänomen würde von heute möglichen Berechnungen unentdeckt bleiben.

F Nullstellenfreie Bereiche von $\zeta(s)$ und das Fehlerglied im Primzahlsatz

Die Kenntnis größerer nullstellenfreier Bereiche von $\zeta(s)$ führt zu besseren Abschätzungen der verschiedenen Funktionen zur Primzahlverteilung.

Wie bereits angedeutet, bestimmte de la Vallée Poussin einen nullstellenfreien Bereich, der an einem wesentlichen Punkt seines Beweises des Primzahlsatzes zur Anwendung kam. Inzwischen gibt es viele Erweiterungen seines Resultats. Ein sehr großer nullstellenfreier Bereich, der hier nicht explizit beschrieben werden soll, wurde von Richert gefunden (und in Walfiszs Buch veröffentlicht, 1963). In einem Vorabdruck von 2001 fand Kadiri (veröffentlicht 2005), dass die folgende Region keine Nullstellen der Riemannschen Zetafunktion enthält:

$$\sigma \geq 1 - \frac{1}{5{,}70233 \log |t|} \quad \text{für} \quad |t| \geq 3\,.$$

Es sei angemerkt, dass es bis heute niemandem gelungen ist, die Existenz eines nullstellenfreien Bereichs von $\zeta(s)$ zu finden, der die Form $\{\sigma + it \mid \sigma \geq \sigma_0\}$ mit $\frac{1}{2} < \sigma_0 < 1$ hat.

Was auch immer über nullstellenfreie Bereiche für $\zeta(s)$ bekannt ist, es lässt sich verwenden, um eine Abschätzung für den Fehler im Primzahlsatz abzuleiten. So ermittelte Tschudakoff (1936)

$$\pi(x) = \mathrm{Li}(x) + O\big(xe^{-C(\log x)^{\alpha}}\big);$$

mit $\alpha < 4/7$ und $C > 0$.

Von Koch zeigte 1901, dass Riemanns Vermutung äquivalent zu folgender Form des Fehlerterms ist:

$$\pi(x) = \mathrm{Li}(x) + O(x^{1/2} \log x).$$

Auch das Wissen, dass sich viele Nullstellen von $\zeta(s)$ auf der kritischen Geraden befinden, führt zu besseren Abschätzungen. So konnten

Rosser & Schoenfeld 1975 beweisen, dass

$$0{,}998684x < \theta(x) < 1{,}001102x$$

(die Abschätzung nach unten ist gültig für $x \geq 1319007$, die nach oben für alle x).

Dusart verwendete 1999 die Kenntnis von 1,5 Milliarden Nullstellen von $\zeta(s)$, um schärfere Abschätzungen zu gewinnen, so zum Beispiel: Für $x > 10544111$,

$$|\theta(x) - x| < 0{,}0066788\frac{x}{\log x}.$$

Ähnliche Abschätzungen für die Funktion $\psi(x)$ stammen von Rosser & Schoenfeld, sowie von Dusart.

Derartige Abschätzungen sind oft Verfeinerungen der Arbeit früherer Autoren, die – wie die Rekordhalter – zeitweilig das beste Ergebnis besaßen. Es wäre daher ungerecht, die Arbeiten von Robin (1983) und von Massias & Robin (1996) unerwähnt zu lassen.

G Einige Eigenschaften von $\pi(x)$

Die erste diesbezügliche Aussage ist, historisch gesehen, Bertrands experimentelle Beobachtung von 1845:

Zwischen $n \geq 2$ und $2n$ gibt es immer eine Primzahl.

Dies lässt sich äquivalent so ausdrücken:

$$\pi(2n) - \pi(n) \geq 1 \quad (\text{für } n \geq 1),$$

oder auch durch

$$p_{n+1} < 2p_n \quad (\text{für } n \geq 1).$$

Diese Aussage ist unter der Bezeichnung „Bertrands Postulat“ bekannt und wurde von Tschebyscheff im Jahre 1852 als Nebenprodukt seiner Abschätzungen für $\pi(x)$ bewiesen. Die kürzesten und vielleicht einfachsten Beweise von Bertrands Postulat stammen von Ramanujan (1919), Erdös (1932) und insbesondere Moser (1949). Die folgenden Ungleichungen geben genauere Auskunft:

$$1 < \frac{1}{3}\,\frac{n}{\log n} < \pi(2n) - \pi(n) < \frac{7}{5}\,\frac{n}{\log n} \quad (\text{für } n \geq 5),$$

es gilt zudem $\pi(4) - \pi(2) = 1$, $\pi(6) - \pi(3) = 1$, $\pi(8) - \pi(4) = 2$.

Allgemeiner bewies Erdös 1949 als Korollar aus dem Primzahlsatz, dass es für jedes $\lambda > 1$ ein $C = C(\lambda) > 0$ und $x_0 = x_0(\lambda) > 1$ derart gibt, dass

$$\pi(\lambda x) - \pi(x) > C\frac{x}{\log x}, \quad \text{für } x \geq x_0.$$

Ich werde mich nun Abschätzungen für $\pi(xy)$ und $\pi(x+y)$ in Abhängigkeit von $\pi(x)$, $\pi(y)$ zuwenden. Das folgende Resultat von Ishikawa (1934) ist eine weitere Konsequenz aus Tschebyscheffs Satz:

Falls $x \geq y \geq 2$, $x \geq 6$, *dann* $\pi(xy) > \pi(x) + \pi(y)$.

Der Vergleich von $\pi(x + y)$ mit $\pi(x)$, $\pi(y)$ ist sehr interessant. Im Jahre 1923 begründeten Hardy & Littlewood aufgrund heuristischer Überlegungen die

Vermutung. $\pi(x + y) \leq \pi(x) + \pi(y)$ *für alle* $x \geq 2$, $y \geq 2$.

Genauer ausgedrückt besagt dies: Für jedes $x > 0$ ist die Anzahl der Primzahlen in jedem Intervall $(y, y+x]$ (ausgenommen y, einschließlich $y + x$) mit beliebigem y höchstens gleich der Anzahl der Primzahlen im Intervall $(0, x]$: $\pi(y + x) - \pi(y) \leq \pi(x)$.

Diese Vermutung erscheint tatsächlich sehr vernünftig, zumindest bestätigt sie die Intuition, dass sich die Primzahlen in höheren Zahlbereichen ausdünnen.

Es sei bemerkt, dass Rosser & Schoenfeld 1975 als Konsequenz aus ihrer scharfen Abschätzung für die Funktion $\theta(x)$ zeigten, dass $\pi(2x) < 2\pi(x)$ für $x \geq 5$. Landau wies die Ungleichung in seiner Abhandlung von 1913 für alle hinreichend großen x nach. Unter Verwendung tiefliegender Methoden konnten Montgomery & Vaughan (1973) beweisen, dass

$$\pi(x + y) \leq \pi(x) + \frac{2y}{\log y}.$$

Wie in Teil E erwähnt, hatten Rosser & Schoenfeld (1975) gezeigt, dass $y/(\log y) < \pi(y)$, daher $\pi(x + y) \leq \pi(x) + 2\pi(y)$.

Der Nachweis der Vermutung von Hardy & Littlewood hat sich als schwieriges Problem herausgestellt. Neben den bereits aufgeführten Ergebnissen bewies Udrescu 1975 in positiver Hinsicht:

Für jedes $\varepsilon > 0$ *gilt: Falls* $x, y \geq 17$ *und* $x + y \geq 1 + e^{4(1+1/\varepsilon)}$, *dann*

$$\pi(x + y) < (1 + \varepsilon)(\pi(x) + \pi(y)).$$

Im Jahre 2002 studierte Dusart die Menge von Paaren (x, y), für die der Ungleichungsfall der Vermutung erfüllt ist. Er bewies:

Für $2 \le x \le y \le (7/5)\, x \log x \log\log x$ *gilt* $\pi(x+y) \le \pi(x) + \pi(y)$.

Es folgt, dass das Verhältnis A/t^2 kleiner als $5/(7 \log t \log\log t)$ ist (für jedes $t > e^{10}$), wobei A die Fläche der Menge aller (x, y) repräsentiert, für die $\pi(x+y) > \pi(x) + \pi(y)$.

In negativer Hinsicht werde ich in Abschnitt IV die Verbindung zwischen der Vermutung von Hardy & Littlewood und der „Primzahlmehrlings-Vermutung“ diskutieren und dabei ihre gegenseitige Unverträglichkeit erläutern.

Zwei weitere Aussagen, die noch auf ihren Beweis warten oder auch widerlegt werden müssen, sind die folgenden:

Opperman behauptete 1882, dass $\pi(n^2+n) > \pi(n^2) > \pi(n^2-n)$ für $n > 1$.

Im Jahre 1904 äußerte Brocard, dass $\pi(p_{n+1}^2) - \pi(p_n^2) \ge 4$ für $n \ge 2$; das heißt, zwischen den Quadraten zweier aufeinander folgender Primzahlen größer als 2 liegen mindestens vier Primzahlen.

Es ist leicht zu sehen, dass sich aus der Vermutung von Opperman die Aussage ableiten lässt, dass es zwischen den Quadraten zweier aufeinander folgender Zahlen mindestens zwei Primzahlen gibt. Dies wiederum würde Brocards Vermutung bestätigen.

H Die Verteilung der Werte von Eulers Funktion

Ich werde an dieser Stelle einige Ergebnisse zur Verteilung der Werte von Eulers Funktion zusammenstellen. Sie ergänzen das, was schon in Kapitel 2, Abschnitt II angegeben wurde.

Zunächst einige Anmerkungen zum Wachstum von Eulers Funktion. Es ist einfach zu zeigen, dass

$$\varphi(n) \ge \log 2 \frac{n}{\log(2n)}\,,$$

insbesondere wächst $\varphi(n)$ für jedes $\delta > 0$ auf jeden Fall schneller als $n^{1-\delta}$. Genauer gibt es sogar für jedes $\varepsilon > 0$ ein $n_0 = n_0(\varepsilon)$ derart, dass wenn $n \ge n_0$, dann

$$\varphi(n) \ge (1-\varepsilon) e^{-\gamma} \frac{n}{\log\log n}\,.$$

Andererseits folgt aus dem Primzahlsatz, dass es unendlich viele n gibt, so dass

$$\varphi(n) < (1+\varepsilon) e^{-\gamma} \frac{n}{\log\log n}\,.$$

Also

$$\liminf \frac{\varphi(n)\log\log n}{n} = e^{-\gamma}.$$

Ein Beweis obiger Resultate findet sich zum Beispiel in den Büchern von Landau (1909) oder Apostol (1976).

Welchen Wert nimmt $\varphi(n)$ im Durchschnitt an?

Aus der Beziehung $n = \sum_{d|n} \varphi(d)$ lässt sich unschwer ableiten, dass

$$\frac{1}{x}\sum_{n\le x} \varphi(n) = \frac{3x}{\pi^2} + O(\log x).$$

Also ist der durchschnittliche Wert von $\varphi(n)$ gleich $3n/\pi^2$.

Als Konsequenz ergibt sich, dass die Wahrscheinlichkeit, dass zwei zufällig gewählte Zahlen m, $n \ge 1$ teilerfremd sind, $6/\pi^2$ beträgt.

Diese Punkte sind in den Büchern von Hardy & Wright und Apostol (1976) sehr gut erklärt.

II Die n-te Primzahl und Lücken zwischen Primzahlen

Die Ergebnisse des vorigen Abschnitts betrafen die Funktion $\pi(x)$, ihr asymptotisches Verhalten, Vergleiche mit bekannten Funktionen und eine Auswahl weiterer Eigenschaften. Es wurden jedoch keine Aussagen über das Verhalten von $\pi(x)$ im Kleinen, über die n-te Primzahl oder auch die Differenz zwischen aufeinander folgenden Primzahlen getroffen. All diese Fragen befassen sich mit den Feinheiten der Verteilung der Primzahlen und lassen viel größere Unregelmäßigkeiten erwarten.

A Die n-te Primzahl

Ich werde nun speziell die n-te Primzahl betrachten.

Aus dem Primzahlsatz folgt unmittelbar:

$$p_n \sim n\log n, \qquad \text{das heißt,} \qquad \lim_{n\to\infty} \frac{p_n}{n\log n} = 1.$$

Mit anderen Worten hat die n-te Primzahl für große Indizes n ungefähr die Größenordnung von $n\log n$. Genauer,

$$p_n = n\log n + n(\log\log n - 1) + O\left(\frac{n\log\log n}{\log n}\right).$$

Für großes n gilt also $p_n > n \log n$. Allerdings bewies Rosser 1938, dass für jedes $n > 1$ gilt:

$$n \log n + n(\log \log n - 10) < p_n < n \log n + n(\log \log n + 8),$$

sowie für jedes $n \geq 1$: $p_n > n \log n$. Dusart zeigte 1999, dass $p_n < n(\log n + \log \log n - 0{,}9484)$ für $n > 39017$ sowie $p_n > n(\log n + \log \log n - 1)$ für alle $n > 1$.

Die folgenden Resultate von Ishikawa (1934) ergeben sich als Konsequenzen aus Tschebycheffs Satz (siehe Trosts Buch, Allgemeine Grundlagen):

Falls $n \geq 2$, dann ist $p_n + p_{n+1} > p_{n+2}$; im Falle $m, n \geq 1$ gilt $p_m p_n > p_{m+n}$.

Dusart gelang es 1998, die Korrektheit der Vermutung von R. Mandl (siehe Rosser & Schoenfeld, 1975) nachzuweisen:

$$\frac{p_1 + p_2 \cdots + p_n}{n} \leq \frac{1}{2} p_n \quad \text{für} \quad n \geq 9.$$

Pomerance betrachtete in einem sehr interessanten Artikel von 1979 den Primzahlgraph, der sich aus allen Punkten (n, p_n) der Ebene (mit $n \geq 1$) zusammensetzt. Er bewies Selfridges Vermutung: Es gibt unendlich viele n mit $p_n^2 > p_{n-i} p_{n+i}$ für alle positiven $i < n$. Zudem existieren unendlich viele n derart, dass $2p_n < p_{n-i} + p_{n+i}$ für alle positiven $i < n$ gilt.

Eine neue, meines Wissens unveröffentlichte Vermutung, die etwa auf das Jahr 1992 zurückgeht, wurde mir von der Autorin F. Firoozbakht mitgeteilt. Sie vermutete, dass die Folge $(p_n^{1/n})_{n \geq 2}$ streng monoton fällt. Eine Vermutung mehr aus der anscheinend unbegrenzten Sammlung plausibler Behauptungen über Primzahlen, sämtlich bis zu hohen Grenzen numerisch verifiziert (ansonsten wären sie wohl im „Mülleimer der Mathematik“ gelandet). Und trotzdem können wir ach so schlauen Mathematiker in so vielen Fällen nicht entscheiden, ob die Aussagen richtig oder falsch sind.

B Lücken zwischen Primzahlen

Der Primzahlsatz gibt Auskunft über das Verhalten der Funktion $\pi(x)$, wenn x ins Unendliche wächst. Um zu einem detaillierteren Verständnis der Verteilung der Primzahlen zu gelangen, ist es notwendig, die Differenzen $d_n = p_{n+1} - p_n$ zwischen aufeinander folgenden Primzahlen zu studieren.

Die *Lücke* nach der Primzahl p ist die Anzahl $g(p)$ zerlegbarer Zahlen, die direkt auf p folgen. Daher $p_{n+1} = p_n + g(p_n) + 1$. Man beachte, dass $g(p)$ für alle $p > 2$ ungerade ist. Die Zahl $g(p_n)$ ist eine *maximale Lücke*, wenn $g(p_n) > g(p_k)$ für alle $p_k < p_n$.

Es sei $G = \{m \mid m = g(p) \text{ für ein } p > 2\}$ die Menge der möglichen Werte von $g(p)$. Für jedes $m \in G$ sei $p[m]$ die kleinste Primzahl p, so dass $g(p) = m$. In der Literatur nennt man $p[m]$ das *erstmalige Auftreten* der Lücke m.

Beim Studium der Lücken, oder gleichbedeutend der Differenz zwischen aufeinander folgenden Primzahlen, sollen die folgenden Themen behandelt werden: Das Verhalten von d_n für n gegen Unendlich, die Menge G möglicher Lücken, das erstmalige Auftreten einer Lücke, die Wachstumsrate von d_n sowie die iterierten Lücken.

Das Verhalten von d_n für n gegen Unendlich

Es ist einfach zu zeigen, dass $\limsup d_n = \infty$. Das heißt, für jedes $N > 1$ gibt es eine Reihe von mindestens N aufeinander folgenden zerlegbaren ganzen Zahlen; zum Beispiel

$$(N+1)!+2,\ (N+1)!+3,\ (N+1)!+4, \ldots, (N+1)!+(N+1).$$

Tatsächlich finden sich Reihen von N zerlegbaren Zahlen experimentell zwischen Zahlen, die viel kleiner sind als $(N+1)!$. Es wäre daher viel beachtlicher, wenn man große Differenzen d_n für kleine n fände – es wäre damit ein größerer „Wert“ im Sinne einer noch zu formulierenden, präziseren Definition verbunden.

Im Gegensatz zu $\limsup d_n$ ist jede Behauptung über $\liminf d_n$ – abgesehen von seiner Existenz – immer noch nicht entschieden. Die denkbaren Möglichkeiten sind:

- $\liminf d_n = \infty$. Dies bedeutet, dass es für jedes k nur endlich viele p_n gibt, für die $d_n = 2k$ ist. Anders ausgedrückt, für jedes k gibt es ein n_0 mit der Eigenschaft: falls $n > n_0$, dann $d_n > 2k$. Richtig oder falsch?
- Es existiert $l \geq 1$ derart, dass $\liminf d_n = l$. Dies bedeutet, dass es unendlich viele Primzahlen p_n gibt, für die $d_n = l$ und l die kleinste Zahl mit dieser Eigenschaft ist. Die Korrektheit dieser Aussage ist für kein l nachgewiesen oder widerlegt.

Diese Fragen sind eng verbunden mit der

Vermutung von Polignac (1849)**.** *Für jede gerade natürliche Zahl $2k$, $k \geq 1$, gibt es unendlich viele aufeinander folgende Primzahlen p_n, p_{n+1}, für die $d_n = p_{n+1} - p_n = 2k$.*

Für den Spezialfall $k = 1$ beinhaltet Polignacs Vermutung die Aussage: Es gibt unendlich viele Primzahlen p derart, dass $p+2$ auch eine Primzahl ist. Dies ist die berühmte *Primzahlzwillingsvermutung*, die in Abschnitt III betrachtet wird.

Man sollte sofort betonen, dass noch nicht einmal die folgende Aussage bewiesen ist: Für jedes $k \geq 1$ gibt es *ein* Paar von Primzahlen p, q, so dass $q - p = 2k$ (ohne zu fordern, dass sie aufeinander folgend sind).

Die Menge G der möglichen Lücken

Das folgende Resultat ist eine einfache Anwendung des Primzahlsatzes und wurde von Powell als Aufgabe im *American Mathematical Monthly* gestellt (1983; Lösung von Davies 1984):

Für jede natürliche Zahl M existiert eine gerade Zahl $2k$ derart, dass es mehr als M Paare aufeinander folgender Primzahlen mit Differenz $2k$ gibt.

Beweis. Für hinreichend großes n betrachte die Folge von Primzahlen

$$3 = p_2 < p_3 < \cdots < p_n$$

und die $n-2$ Differenzen $p_{i+1} - p_i$ $(i = 2, \ldots, n-1)$. Falls die Anzahl der verschiedenen Differenzen kleiner ist als

$$\left[\frac{n-2}{M}\right],$$

so taucht eine der Differenzen, etwa $2k$, mehr als M mal auf. Im anderen Fall ist

$$p_n - p_2 \geq 2 + 4 + \cdots + 2\left[\frac{n-2}{M}\right].$$

Aber die rechte Seite ist asymptotisch gleich n^2/M^2, während die linke Seite nach dem Primzahlsatz asymptotisch gleich $n \log n$ ist, was nicht sein kann. □

Obiges Ergebnis kann man auch so ausdrücken: Für jede natürliche Zahl M existiert eine ungerade Zahl $m \in G$ derart, dass $g(p) = m$ für mehr als M Primzahlen p gilt.

Es ist unbekannt, ob jede gerade, positive Zahl als Differenz zwischen zwei aufeinander folgenden Primzahlen auftritt – dies wurde bereits in

Verbindung mit Polignacs Vermutung erwähnt. Man weiß also nicht, ob G identisch mit der Menge aller ungeraden positiven Zahlen ist.

Es hat große Bemühungen gegeben, bis zu einer bestimmten Obergrenze Lücken (zwischen angemessen „kleinen“ Primzahlen) für jede vorgegebene Länge zu finden. Andererseits richten sich die Anstrengungen darauf, außergewöhnlich große Lücken zwischen Primzahlen ausfindig zu machen.

Dubner entwickelte einen Algorithmus, der es ihm 2002 ermöglichte, für jedes ungerade $m < 10180$ eine Primzahl p zu bestimmen, auf die genau m zerlegbare Zahlen folgen. In diesem Bereich ergaben sich Primzahlen p als obere Schranken für $p[m]$, die bis zu 398 Stellen hatten.

In neuerer Zeit sind diese Ergebnisse deutlich übertroffen worden. T. Alm und J.K. Andersen fanden Lücken für jede Länge $m < 18000$, wobei in dem von Dubner abgedeckten Bereich die jeweiligen Primzahlen p erheblich kleiner waren. Darüber hinaus bestimmten sie für alle weiteren m mit $m < 32000$ Lücken, die oft nur noch der Bestätigung bedürfen, dass die Quasiprimzahl, welche die Lücke nach oben begrenzt, wirklich prim ist.

Rekord

Die größte explizit bestimmte Lücke zwischen zwei unmittelbar aufeinander folgenden Primzahlen besteht aus einer Reihe von 383795 zerlegbaren Zahlen, die auf die 7183-stellige Primzahl $9527\times(16673\#)/2310-175622$ folgen. Diese Lücke wurde im März 2010 von P. Cami identifiziert, der bald darauf mit Hilfe des ECPP-Programms von M. Martin auch die Primalität der beiden Endzahlen nachwies.

Bereits 2004 hatten H. Rosenthal und J.K. Andersen eine Lücke zwischen zwei 86853-stelligen Quasiprimzahlen entdeckt, die durch 2254929 zerlegbare Zahlen voneinander getrennt sind. Wenn es einmal gelingen sollte, die beiden begrenzenden Zahlen als Primzahlen zu bestätigen, hätte man hiermit eine *Megalücke* bestimmt (eine Lücke mit einer Länge von mehr als einer Million).

Das erstmalige Auftreten und der Wert einer Lücke

In der Vergangenheit wurden immer umfangreichere Tabellen mit Werten von $p[m]$ erstellt, aus denen sich ablesen lässt, welches die Primzahlen sind, auf die maximale Lücken folgen. In der Reihenfolge ihres Erscheinens: Lander & Parkin (1967), Brent (1973, 1980), Young & Potler (1989) und Nicely (1999). Die Berechnungen wurden von Nicely und

T. Oliveira e Silva fortgeführt, in Zusammenarbeit mit B. Nyman und S. Herzog. Im August 2010 waren alle Primzahlen bis $N = 1{,}6 \times 10^{18}$ untersucht.

Rekord

Für $p < N$ beträgt die größte bekannte maximale Lücke $m = 1475$, wobei $p[1475] = 1425172824437699411$. Sie wurde von Oliveira e Silva im April 2009 entdeckt. Zuvor war sein früherer Rekord aus dem Jahre 2002, mit $m = 1197$, weitere sieben Male übertroffen worden, zumeist von ihm selbst und zweimal durch D.E. Knuth. Davor hatte Nyman die Werte $m = 1183$ (2002) und $m = 1131$ (1999) bestimmt. Frühere maximale Lücken hatten $m = 803$, gefunden von Young & Potler (1989), sowie $m = 651$, von Brent (1973).

Wenn im Rahmen bestehender Tabellen m nicht als Funktionswert $g(p)$ erscheint, dann lässt sich ohne weitere Untersuchungen nicht viel sagen. Die kleinste Lücke mit ungewissem erstmaligen Auftreten ist $m = 1263$. Die bislang beste obere Schranke $1798556720194308703 \geq p[1263]$ wurde von C. Kern und Oliveira e Silva angegeben.

Bezüglich des asymptotischen Verhaltens von $p[m]$ stellte Shanks 1964 die Vermutung auf, dass $\log p[m] \sim \sqrt{m}$ (wenn m gegen Unendlich läuft). Auf eigenen, umfangreichen Berechnungen basierend vermutete Weintraub 1991, dass

$$\log p[m] \sim \sqrt{1{,}165746\, m}.$$

Wenn man die auf eine Primzahl p folgende Lücke $g(p)$ bestimmt hat (die nicht notwendigerweise erstmalig auftreten muss), liegt es nahe sich zu fragen, inwieweit diese Lücke im Vergleich zu Primzahlen gleicher Größenordnung „ungewöhnlich groß“ ist. Aus dem Primzahlsatz folgt, dass die durchschnittliche Lücke zwischen Primzahlen in der Nähe von p etwa gleich $\log p$ ist. Der *Wert* einer Lücke $g(p)$ ist definiert als $g(p)/\log p$: Je größer ihr Wert, desto ungewöhnlicher die Lücke.

Die Lücke mit dem größten bekannten Wert, der 35,29 beträgt, ist die oben genannte maximale Lücke mit $g(p) = 1475$. Als nächstes folgt die Primzahl $p = 804212830686677669$ mit $g(p) = 1441$ und dem Wert 34,95. Diese Lücke wurde von Herzog und Oliveira e Silva entdeckt. Zum Vergleich: Die größte bekannte Lücke mit der Länge 383795 hat einen Wert von 23,20 und die vermeintliche Megalücke, die oben genannt wurde, würde den Wert 11,27 haben.

Die Wachstumsrate von d_n

Die Grundidee dieser Untersuchung ist einfach: Funktionen $f(p_n)$ mit reellen, positiven Werten zu finden, die einfach, leicht zu berechnen und mit d_n vergleichbar sind. Gewöhnlich enthält $f(p_n)$ Potenzen oder Logarithmen und der Vergleich dreht sich um Fragen wie:

$$\text{Ist } d_n = O(f(p_n))\,? \quad \text{Ist } d_n = o(f(p_n))\,? \quad \text{Ist } d_n \sim f(p_n)\,?$$

Zunächst besagt das alte Resultat von Tschebyscheff über Bertrands Postulat, dass $d_n < p_n$ für jedes $n \geq 1$.

Nach dem Primzahlsatz gilt

$$\lim_{n\to\infty} \frac{d_n}{p_n} = 0.$$

Offensichtlich ist $d_n = O(p_n)$, da $d_n < p_n$ für jedes $n \geq 1$. Es stellt sich die Frage nach der besten Funktion $f(p_n)$, die $d_n = O(f(p_n))$ erfüllt.

Die Mathematiker hoffen, ohne die Voraussetzung der Riemannschen Vermutung beweisen zu können, dass $d_n = O(p_n^{(1/2)+\varepsilon})$ für jedes $\varepsilon > 0$. Beim Wettlauf, diese Schranke zu erreichen, sind die Fortschritte nur geringfügig, beginnend mit Hoheisel (1930), der $d_n = O(p_n^{\theta})$ mit einem θ knapp unterhalb 1 zeigte, über Artikel von Ingham (1937), Montgomery (1969), Huxley (1972), Iwaniec & Jutila (1979), Heath-Brown & Iwaniec (1979), Iwaniec & Pintz (1984), bis zu den Rekorden aus jüngerer Zeit.

Rekord

Den gegenwärtigen Rekord von $\theta = 0{,}525$ teilen sich Baker, Harman & Pintz (2001). Mozzochi erreichte im Jahre 1986 $\theta = 1051/1920 \approx 0{,}5474$, während Lou & Yao 1993 mit $\theta = 6/11 \approx 0{,}5454$ knapp darunter bleiben konnten.

Die vorangegangenen Ergebnisse liefern Aussagen über das Verhalten von d_n für wachsendes n. Im Gegensatz dazu geben Berechnungen von Ramaré & Saouter (2003) die beruhigende Gewissheit, dass sich in bestimmten, kurzen Intervallen mindestens eine Primzahl befindet. Es sei $x_0 = 10\,726\,905\,041$ und $\Delta = 28\,314\,000$. Für n mit $p_n > x_0$ gilt $d_n < p_{n-1}/\Delta$.

Unter Annahme der Richtigkeit der Riemannschen Vermutung zeigte Cramér 1937, dass $d_n = O(p_n^{1/2} \log p_n)$. Auf probabilistischen Betrachtungen basierend vermutete Cramér, dass $d_n = O((\log p_n)^2)$.

Im Zusammenhang mit ungewöhnlich kleinen Lücken erzielte man die folgenden Ergebnisse. Zunächst bewies Erdös 1940 die Existenz einer Konstanten C mit $0 < C < 1$, so dass gilt

$$\liminf \frac{d_n}{\log p_n} < C.$$

Der Wert von C wurde verschiedentlich abgeschätzt. Bombieri & Davenport zeigten 1966, dass man C gleich 0,467 wählen kann. Dies wurde zunächst von Huxley (1977), dann von Maier (1985) verbessert, der für die Konstante 0,248 setzen konnte. Den Durchbruch schafften erst kürzlich Goldston, Pintz & Yıldırım (2005, veröffentlicht 2009), denen es gelang zu beweisen, dass der Grenzwert tatsächlich gleich 0 ist.

In Bezug auf ungewöhnlich große Lücken bewies Westzynthius 1931, dass $\limsup(d_n/\log p_n) = \infty$, das heißt, es gibt für jedes $t > 0$ unendlich viele $n > 0$ mit $p_{n+1} > p_n + t \log p_n$.

Im Jahre 1938 begann Rankin damit, die vorausgegangene Arbeit von Erdös (1935) fortzuführen und bewies 1963 das schärfere Resultat: Es gibt unendlich viele n derart, dass

$$\frac{d_n}{\log p_n} \geq l_n e^{\gamma} = l_n \times 1{,}78107\ldots,$$

wobei γ die Eulersche Konstante ist und

$$l_n = \frac{(\log_2 p_n)(\log_4 p_n)}{(\log_3 p_n)^2} > 1.$$

Erdös hatte einen Preis von 10000 US-Dollar für den Beweis ausgesetzt, dass man in der Erdös-Rankin-Ungleichung e^{γ} durch ∞ ersetzen kann. Leider ist es seit 1996 sehr viel schwieriger geworden, den Gewinn einzulösen.

Ein weiteres offenes Problem ist der Nachweis von

$$\lim_{n\to\infty} \left(\sqrt{p_{n+1}} - \sqrt{p_n}\right) = 0.$$

Es ist leicht zu zeigen, dass die Richtigkeit dieser Vermutung die folgende Aussage zur Folge hätte: Für jede natürliche Zahl M und genügend großes N gibt es mindestens M Primzahlen zwischen N^2 und $(N+1)^2$.

D. Andrica stellte 1986 die verwandte Vermutung auf: $\sqrt{p_{n+1}} - \sqrt{p_n} < 1$ für alle $n \geq 1$. Falls sich Oppermans Vermutung als richtig

herausstellt, dann gilt auch die von Andrica: Denn sei N für gegebenes p_n die größte Zahl mit $N^2 < p_n$, also $p_n < (N+1)^2$. Aus Oppermans Vermutung folgt $p_{n+1} < (N+1)^2$ und insgesamt $\sqrt{p_{n+1}} - \sqrt{p_n} < (N+1) - N = 1$.

Es ist nicht allzu schwierig, die Vermutung von Andrica bis in höhere Bereiche direkt zu überprüfen. Dies ist in der Tat bis $2^{42} \approx 4{,}39 \times 10^{12}$ geschehen. Es ist aber auch darauf hingewiesen worden, dass die obige Ungleichung gleichbedeutend mit $g(p_n) < 2\sqrt{p_n}$ ist, wobei $g(p_n)$ die Lücke zwischen p_n und p_{n+1} bezeichnet. Daher ist auch leicht einzusehen, dass es ausreicht, die letztere Ungleichung nur für die maximalen Lücken unterhalb einer gegebenen Grenze N zu verifizieren, um Andricas Ungleichung für alle $p_n < N$ nachzuweisen. Unter Verwendung der vorhandenen Liste des ersten Auftretens von Lücken, die von Nicely, Oliveira e Silva, Nyman und Herzog erstellt wurde, ist dies für $N = 1{,}6 \times 10^{18}$ schnell getan.

Die Implikationen (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) zwischen den folgenden Aussagen sind leicht zu beweisen:

(i) Es existieren mindestens zwei Primzahlen zwischen den Quadraten aufeinander folgender Zahlen (wie schon erwähnt, folgt (i) aus Oppermans Vermutung).

(ii) Andricas Vermutung.

(iii) Es existiert mindestens eine Primzahl zwischen den Quadraten zweier aufeinander folgender Zahlen.

Aussage (iii) scheint tatsächlich wahr zu sein, muss aber noch bewiesen werden.

Die iterierten Lücken

Proth befasste sich 1878 mit iterierten Lücken zwischen Primzahlen. Es sei $p_1 = 2$, $p_2 = 3$, …, p_n, $p_{n+1}, \ldots$ die Folge der Primzahlen und $\delta_1(n) = |p_{n+1} - p_n| = d_n$ für $n \geq 1$. Allgemeiner sei für $k \geq 1$ $\delta_{k+1}(n) = |\delta_k(n+1) - \delta_k(n)|$. Man erhält so die folgende Sequenz:

2	3	5	7	11	13	17	19	23	29	...
1	2	2	4	2	4	2	4	6		
1	0	2	2	2	2	2	2			
1	2	0	0	0	0	0				
1	2	0	0	0	0					
1	2	0	0	0						
1	2	0	0							
1	2	0								etc.

Für jedes k in dieser Tabelle, $1 \le k \le 7$, ist $\delta_k(1) = 1$. Proth behauptete, nachgewiesen zu haben, dass $\delta_k(1) = 1$ für jedes $k \ge 1$ gilt, sein Beweis war allerdings falsch. N.L. Gilbreath formulierte in den 1950er Jahren in Unkenntnis von Proths Arbeit dieselbe Aussage als Vermutung (unveröffentlicht). Killgrove & Ralston prüften diese 1959 für $k \le 63419$. Odlyzko verifizierte 1993, dass $\delta_k(1) = 1$ für alle $k \le 3{,}46 \times 10^{11}$ gilt, mit anderen Worten, dass die Vermutung für alle Primzahlen bis 10^{13} richtig ist.

III Primzahlzwillinge

Wenn sowohl p als auch $p+2$ Primzahlen sind, nennt man sie *Primzahlzwillinge*.

Die kleinsten Paare von Primzahlzwillingen sind $(3,5)$, $(5,7)$, $(11,13)$ und $(17,19)$. Primzahlzwillinge wurden von Clement im Jahre 1949 wie folgt charakterisiert.

Es sei $n \ge 2$. Die Zahlen n, $n+2$ bilden genau dann ein Paar von Primzahlzwillingen, wenn

$$4\big[(n-1)!+1\big] + n \equiv 0 \pmod{n(n+2)}.$$

Beweis. Wenn die Kongruenz erfüllt ist, dann ist $n \ne 2$, 4 und

$$(n-1)!+1 \equiv 0 \pmod{n},$$

so dass nach Wilsons Satz n eine Primzahl ist. Zudem gilt

$$4(n-1)!+2 \equiv 0 \pmod{n+2};$$

multipliziert mit $n(n+1)$,

$$4\big[(n+1)!+1\big] + 2n^2 + 2n - 4 \equiv 0 \pmod{n+2};$$

daraus folgt

$$4\big[(n+1)!+1\big]+(n+2)(2n-2)\equiv 0 \pmod{n+2};$$

und nach Wilsons Satz ist auch $n+2$ prim.

Umgekehrt, falls n, $n+2$ Primzahlen sind, ist $n\neq 2$ und

$$\begin{aligned}(n-1)!+1&\equiv 0 \pmod{n},\\ (n+1)!+1&\equiv 0 \pmod{n+2}.\end{aligned}$$

Aber $n(n+1)=(n+2)(n-1)+2$, also $2(n-1)!+1=k(n+2)$, wobei k eine ganze Zahl ist. Aus $(n-1)!\equiv -1 \pmod{n}$ folgt $2k+1\equiv 0 \pmod{n}$, dies eingesetzt liefert $4(n-1)!+2\equiv -(n+2) \pmod{n(n+2)}$ und daher schließlich $4[(n-1)!+1]+n\equiv 0 \pmod{n(n+2)}$. □

Allerdings hat diese Charakterisierung keinen praktischen Wert bei der Bestimmung von Primzahlzwillingen.

Das Hauptproblem besteht darin festzustellen, ob es unendlich viele Primzahlzwillinge gibt.

Brun bewies 1919 das berühmte Resultat, dass die Summe

$$\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\cdots+\left(\frac{1}{p}+\frac{1}{p+2}\right)+\cdots,$$

über alle Primzahlen p, für die auch $p+2$ prim ist, gegen eine Zahl B konvergiert, die man heute als *Brunsche Konstante* bezeichnet.

Dieses Ergebnis beinhaltet nicht die Existenz unendlich vieler Paare von Primzahlzwillingen, sagt aber aus, dass sie sich immer weiter voneinander entfernen und so die Summe ihrer Reziproken endlich bleibt.

Auf der Grundlage heuristischer Überlegungen zur Verteilung von Primzahlzwillingen wurde B näherungsweise berechnet, zum Beispiel von Shanks & Wrench (1974), Brent (1976), und in neuerer Zeit von Nicely (2001) und von P. Sebah (2002), der den folgenden Wert ermittelte:

$$B = 1{,}902160583104\ldots.$$

Brun bewies außerdem, dass es für jedes $m\geq 1$ eine Reihe von m aufeinander folgenden Primzahlen gibt, die keine Primzahlzwillinge sind.

Für jedes $x>1$ bezeichne $\pi_2(x)$ die Anzahl der Primzahlen p, für die auch $p+2$ eine Primzahl ist und für die $p\leq x$ gilt.

Brun verkündete 1919 die Existenz einer effektiv berechenbaren Zahl x_0 mit der Eigenschaft, dass für $x \geq x_0$,

$$\pi_2(x) < \frac{100x}{(\log x)^2}\,.$$

Der Beweis erschien 1920.

Die obere Schranke für $\pi_2(x)$ wurde durch die Bestimmung der Konstanten und der Größe des Fehlers reduziert, unter anderem durch Bombieri & Davenport (1966). Es handelt sich bei dieser Arbeit um eine Anwendung von Siebmethoden, der Beweis findet sich zum Beispiel im Buch von Halberstam & Richert.

Hier das Ergebnis:

$$\pi_2(x) \leq 2C \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \frac{x}{(\log x)^2}\,.$$

Die bislang besten Werte, die man für C erreichte, waren $C = 3{,}5$ von Bombieri, Friedlander & Iwaniec (1986) und $C = 3{,}13$ von S. Lou (persönliche Mitteilung).

Bereits früher hatten Hardy & Littlewood (1923) aufgrund heuristischer Überlegungen vermutet, dass

$$\pi_2(x) \sim 2C_2 \frac{x}{(\log x)^2},$$

wobei man das unendliche Produkt

$$C_2 = \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right)$$

(siehe Kapitel 6, Abschnitt IV) die *Primzahlzwillingskonstante* nennt. Ihr Wert ist 0,66016... und wurde von Wrench 1961 berechnet.

Um die Konstante C_2 auszurechnen, wurde die heuristische Argumentation von Hardy und Littlewood im Verlauf der Zeit von anderen Autoren erläutert, eine einfache Erklärung stammt von Golomb (1960). Es ist nicht uninteressant, den Gedankengang hin zur Konstanten C_2 zu beschreiben, auch wenn die Argumentation noch nicht in aller Strenge geführt werden kann.

Der Primzahlsatz besagt, dass $\pi(x)/x \sim 1/(\log x)$, daher ist die Wahrscheinlichkeit, dass die positive ganze Zahl n eine Primzahl ist, gleich $1/(\log n)$, und im Wesentlichen gilt dies auch für $n+2$. Wenn also die beiden Ereignisse unabhängig voneinander wären, ergäbe sich

für die Wahrscheinlichkeit, dass sowohl n als auch $n+2$ Primzahlen sind, der Wert $1/(\log n)^2$. Aber die Ereignisse sind nicht unabhängig. Wenn n eine Primzahl ist und $n > 2$, dann ist n ungerade. Dies gilt dann auch für $n+2$ und daher muss die Wahrscheinlichkeit für $n+2$ verdoppelt werden, um der Tatsache gerecht zu werden, dass $n+2$ Element der Teilmenge der ungeraden Zahlen ist.

Für jede ungerade Primzahl $p \neq n$ gehört die Zahl n einer der $(p-1)/p$ Restklassen an; wenn $n+2$ auch eine Primzahl ist und nicht von p geteilt wird, dann gehört sie zu einer der $(p-2)/(p-1)$ vorangegangenen Klassen. Auf diese Weise muss man für jede Primzahl $p > 2$ einen Faktor

$$\frac{p-2}{p-1}\Big/\frac{p-1}{p} = \frac{p(p-2)}{(p-1)^2} = 1 - \frac{1}{(p-1)^2}$$

in die Berechnung der Wahrscheinlichkeit einbeziehen, die aufgrund dieser heuristischen Überlegungen gleich $C_2/(\log n)^2$ ist.

Um ein Gefühl für das Wachstum von $\pi_2(x)$ zu vermitteln, gebe ich in Tabelle 16 die wichtigsten Stufen der Berechnungen von Brent (1975, 1976), Nicely (1995, 2001), P. Sebah und P. Demichel (2002) sowie T. Oliveira e Silva (2004, 2008) wieder. Letzterer erstellte zudem die umfangreichsten Tabellen mit Werten von $\pi_2(x)$, die bisher bekannt sind. Die Werte bis $x = 10^{16}$ wurden später von Nicely verifiziert.

Tabelle 16. Anzahl der Primzahlzwillinge

x	$\pi_2(x)$
10^3	35
10^4	205
10^5	1 224
10^6	8 169
10^7	58 980
10^8	440 312
10^9	3 424 506
10^{10}	27 412 679
10^{11}	224 376 048
10^{12}	1 870 585 220
10^{13}	15 834 664 872
10^{14}	135 780 321 665
10^{15}	1 177 209 242 304
10^{16}	10 304 195 697 298
10^{17}	90 948 839 353 159
10^{18}	808 675 888 577 436

Rekord

Der größte genaue Wert der Anzahl von Primzahlzwillingen unterhalb einer gegebenen Grenze wurde von Oliveira e Silva bestimmt, der bis Anfang 2010 folgenden Wert erreicht hatte:

$$\pi_2(1{,}6 \times 10^{18}) = 1\,264\,267\,586\,627\,937.$$

Rekorde

In der folgenden Tabelle sind die größten bekannten Primzahlzwillingspaare aufgeführt.

Tabelle 17. Die größten bekannten Primzahlzwillingspaare

Primzahlpaar	Stellen	Entdecker	Jahr
$65516468355 \times 2^{333333} \pm 1$	100355	P. Kaiser, K. Klahn, P. Jobling, J. Penné und PrimeGrid	2009
$2003663613 \times 2^{195000} \pm 1$	58711	E. Vautier, P.W. McKibbon, D. Gribenko, M. Kwok, P. Jobling, J. Penné u. a.	2007
$194772106074315 \times 2^{171960} \pm 1$	51780	Z. und A. Járai, G. Farkas, T. Csajbok und J. Kasza	2007
$100314512544015 \times 2^{171960} \pm 1$	51780	Z. und A. Járai, G. Farkas, T. Csajbok und J. Kasza	2006
$16869987339975 \times 2^{171960} \pm 1$	51779	Z. und A. Járai, G. Farkas, T. Csajbok und J. Kasza	2005
$33218925 \times 2^{169690} \pm 1$	51090	D. Papp, P. Jobling, G. Woltman und Y. Gallot	2002
$8151728061 \times 2^{125987} \pm 1$	37936	D. Augustin, P. Jobling und J. Penné	2010
$598899 \times 2^{118987} \pm 1$	35825	T. Wu und J. Penné	2010
$307259241 \times 2^{115599} \pm 1$	34808	B. Tornberg, P. Jobling, G. Woltman und Y. Gallot	2009
$60194061 \times 2^{114689} \pm 1$	34533	D. Underbakke, G. Woltman und Y. Gallot	2002

Eine Menge von $2k$ aufeinander folgenden Primzahlen, die aus k Paaren von Primzahlzwillingen besteht, nennt man eine *Häufung von Primzahlzwillingen der Ordnung k*. Die Existenz solcher Häufungen von Primzahlzwillingen beliebiger Ordnung ist niemals bewiesen worden, sie folgt jedoch aus der unbewiesenen Vermutung von Dickson;

siehe Kapitel 6, Abschnitt I, (D_3). N.B. Backhouse teilte mir 1996 die ersten Häufungen von Primzahlzwillingen (d. h. jene mit kleinster Anfangsprimzahl) der Ordnungen 1 bis 7 mit. Sie beginnen mit den Primzahlen 3, 5, 5, 9419, 909 287, 325 267 931 beziehungsweise 678 771 479.

Rekorde

Für die nächsten Ordnungen beginnt die erste Häufung von Primzahlzwillingen jeweils mit der folgenden der Primzahl:

Ordnung 8:	1 107 819 732 821,	P. Carmody 2001,
Ordnung 9:	170 669 145 704 411,	D. DeVries und P. Sebah 2002,
Ordnung 10:	3 324 648 277 099 157,	G. Lévai 2004.

Viele Autoren haben versucht, mit Hilfe von Siebmethoden zu beweisen, dass es unendlich viele Primzahlzwillinge gibt.

Zunächst zeigte Brun in seinem berühmten Artikel von 1920, dass sich die Zahl 2 auf unendlich viele Weisen in der Form $2 = m - n$ schreiben lässt, wobei m, n Produkte von höchstens 9, nicht notwendigerweise verschiedenen Primzahlen sind.

Das bis heute beste mit Siebmethoden gewonnene Resultat stammt von Chen (angekündigt 1966, veröffentlicht 1973, 1978); er zeigte, dass sich die 2 auf unendlich viele Weisen in der Form $2 = m - p$ darstellen lässt, wobei p eine Primzahl und m ein Produkt von höchstens zwei nicht notwendigerweise verschiedenen Primzahlen ist.

Die beim Studium der Primzahlzwillinge verwendeten Siebmethoden eignen sich auch zur Untersuchung der Goldbachschen Vermutung (siehe Abschnitt VI).

Die allgemeine Polignac-Vermutung (siehe letzter Abschnitt) kann teilweise wie die Primzahlzwillingsvermutung behandelt werden.

Für jedes $k \geq 1$ und $x > 1$ bezeichne $\pi_{2k}(x)$ die Anzahl der Zahlen $n > 1$, für die $p_{n+1} \leq x$ und $p_{n+1} - p_n = 2k$.

Mit Hilfe der Methode von Brun lässt sich die Existenz einer Konstanten $C_k > 0$ nachweisen, so dass

$$\pi_{2k}(x) < C_k \frac{x}{(\log x)^2} .$$

Ein wichtiger Fortschritt hin zu einem Beweis der Primzahlzwillingsvermutung ist die bereits zuvor erwähnte neue Arbeit von Goldston, Pintz & Yıldırım (2009); siehe auch Goldston, Motohashi, Pintz & Yıldırım (2006).

Unter der Voraussetzung einer Vermutung von Elliott und Halberstam wird gezeigt, dass es unendlich viele Paare aufeinander folgender Primzahlen mit einer Differenz von höchstens 16 gibt.

IV Primzahlmehrlinge

Oben habe ich Paare von Zwillingsprimzahlen $(p, p+2)$ betrachtet. Sie bestehen aus zwei aufeinander folgenden Primzahlen mit der kleinstmöglichen Differenz 2.

In ähnlicher Weise werden nun *Primzahldrillinge* (p_0, p_1, p_2) definiert, wobei $p_0 < p_1 < p_2$ aufeinander folgende Primzahlen mit der kleinstmöglichen Differenz $p_2 - p_0$ sind. Es gibt zwei Arten von Primzahldrillingen: $(p, p+2, p+6)$, wie zum Beispiel $(11, 13, 17)$, und $(p, p+4, p+6)$, wie $(7, 11, 13)$. Es ist klar, dass wenn p, $p+2$, $p+4$ prim sind, $p = 3$ ist, denn eine der drei Zahlen muss durch 3 teilbar sein.

Das Quadrupel (p_0, p_1, p_2, p_3) nennt man *Primzahlvierling*, wenn $p_0 < p_1 < p_2 < p_3$ aufeinander folgende Primzahlen sind und $p_3 - p_0$ kleinstmöglich ist. Da p, $p+2$, $p+4$, $p+6$ nicht sämtlich Primzahlen sein können, ist die kleinstmögliche Differenz nicht 6. Aber 11, 13, 17, 19 sind alle prim, so dass die Mindestdifferenz 8 beträgt und $(11, 13, 17, 19)$ ein Primzahlvierling ist. Wie jeder andere Primzahlvierling hat er die Form $(p, p+2, p+6, p+8)$ mit einer Primzahl p.

Allgemeiner sei $k \geq 2$ und

(i) $b_1 < b_2 < \cdots < b_{k-1}$,

(ii) $p, p+b_1, \ldots, p+b_{k-1}$ seien k aufeinander folgende Primzahlen,

(iii) es sei angenommen, dass es keine Folge von Primzahlen $q_0 < q_1 < \cdots < q_{k-1}$ mit $q_{k-1} - q_0 < b_{k-1}$ gibt.

Dann nennt man $(p, p+b_1, \ldots, p+b_{k-1})$ einen *Primzahlmehrling der Ordnung* k und $(b_1, b_2, \ldots, b_{k-1})$ den *Typ* des Primzahlmehrlings.

Ich führe nun folgende Bezeichnungen ein: Für jedes reelle $x > 0$ sei

$$\pi_{2,6}(x) = \#\{(p, p+2, p+6) \mid (p, p+2, p+6) \text{ ist ein Primzahldrilling und } p \leq x\},$$
$$\pi_{4,6}(x) = \#\{(p, p+4, p+6) \mid (p, p+4, p+6) \text{ ist ein Primzahldrilling und } p \leq x\}.$$

In ähnlicher Weise sei

$$\pi_{2,6,8}(x) = \#\{(p, p+2, p+6, p+8) \mid (p, p+2, p+6, p+8) \text{ ist ein Primzahlvierling und } p \le x\}.$$

Zudem seien

$$B_{2,6} = \sum \left(\frac{1}{p} + \frac{1}{p+2} + \frac{1}{p+6}\right),$$
$$B_{4,6} = \sum \left(\frac{1}{p} + \frac{1}{p+4} + \frac{1}{p+6}\right),$$
$$B_{2,6,8} = \sum \left(\frac{1}{p} + \frac{1}{p+2} + \frac{1}{p+6} + \frac{1}{p+8}\right),$$

wobei sich die Summation über alle Drillinge (bzw. Vierlinge) des jeweils angezeigten Typs erstreckt. Genau wie im Falle von Bruns Resultat über die Reziproken der Zwillingsprimzahlen $(p, p+2)$ sind auch alle oben angegebenen Summen konvergent, was natürlich nicht im Widerspruch zur Möglichkeit steht, dass es von den jeweiligen Primzahlmehrlingen unendlich viele gibt.

Rekorde

Die folgenden Werte wurden von T.R. Nicely im September 2009 mitgeteilt. Für $N = 2 \times 10^{16}$ ist

$$\pi_{2,6}(N) = 1\,178\,112\,426\,442,$$
$$\pi_{4,6}(N) = 1\,178\,110\,447\,049,$$
$$\pi_{2,6,8}(N) = 46\,998\,268\,431.$$

Rekorde

Die nachfolgend angegebenen Beispiele größter bekannter Primzahlmehrlinge der Ordnung k (mit $k \ge 3$) sind einer Liste entnommen, die von T. Forbes geführt wird.

(1) Drilling $(p, p+2, p+6)$ mit $p = 2072644824759 \times 2^{33333} - 1$ (10047 Stellen, N. Luhn und F. Morain, 2008).

(2) Drilling $(p, p+4, p+6)$ mit
$p = (99241437759 \times d(d+1) + 210)(d-1)/35 + 1$,
wobei $d = 205881 \times 4001\#$
(5132 Stellen, K. Davis u. a., 2006).

(3) Vierling $(p, p+2, p+6, p+8)$ mit
$p = 4104082046 \times 4799\# + 5651$
(2058 Stellen, N. Luhn und M. Martin, 2005).

(4) Fünfling $(p, p+4, p+6, p+10, p+12)$ mit
$p = 424232794973 \times 2593\# + 43777$
(1107 Stellen, N. Luhn und M. Martin, 2009).

Zur Veranschaulichung dessen, wie weit solche Berechnungen getrieben worden sind, sei hier der größte bekannte Primzahlmehrling der Ordnung 17 vorgestellt:

$$(p, p+6, p+8, p+12, p+18, p+20, p+26, p+32, p+36,$$
$$p+38, p+42, p+48, p+50, p+56, p+60, p+62, p+66),$$
$$\text{mit } p = 224989581869473883242253471$$

(27 Stellen, J. Wróblewski im Juni 2010).

Wie angedeutet, sind für kleines k viele Primzahlmehrlinge der Ordnung k bekannt. Im Falle sehr großer k stellt sich jedoch die Frage, wie man überhaupt einen Primzahlmehrling dieser Ordnung finden soll. Was kann man tun, wenn $k = 10^{10^{10}}$? Wie ist es möglich festzustellen, ob es dann einen Primzahlmehrling gibt? Dieser sehr interessanten Frage werde ich mich jetzt etwas detaillierter zuwenden.

Es sei $k \geq 2$. Ein $(k-1)$-Tupel $(b_1, b_2, \ldots, b_{k-1})$ von ganzen Zahlen heißt *zulässig*, wenn

(i) $b_1 < b_2 < \cdots < b_{k-1}$,

(ii) für jede Primzahl $q \leq k$ ist die Menge der Restklassen $\{0 \bmod q, b_1 \bmod q, b_2 \bmod q, \ldots, b_{k-1} \bmod q\}$ echt in der Menge aller Restklassen modulo q enthalten.

Falls $(b_1, b_2, \ldots, b_{k-1})$ zulässig ist, führt die Wahl von $q = 2$ dazu, dass alle b_i gerade sind. Unter den zulässigen $(k-1)$-Tupeln heißen solche mit minimalem b_{k-1} *dicht*. Für $k \leq 4$ sind die folgenden zulässigen $(k-1)$-Tupel dicht: (2), $(2,6)$, $(4,6)$ und $(2,6,8)$.

Nach Hensley & Richards (1974) und der von ihnen verwendeten Bezeichnungsweise sei $\rho^*(x) = k$, falls es ein zulässiges $(k-1)$-Tupel $(b_1, b_2, \ldots, b_{k-1})$ mit $b_{k-1} < x$ gibt, aber kein solches mit mehr als $k-1$ Komponenten. Die Berechnung von $\rho^*(x)$ kann für jedes x in endlich vielen Schritten durchgeführt werden, für großes x ist dies jedoch ein kompliziertes kombinatorisches Problem.

Ähnliche Funktionen tauchen in der Literatur unter anderem bei Hardy & Littlewood (1923), Schinzel & Sierpiński (1958) sowie bei weiteren Autoren auf. Insbesondere

$$\rho(x) = \limsup_{y\to\infty} \big(\pi(x+y) - \pi(y)\big).$$

Es gilt $\rho(x) \le \rho^*(x)$.

Beweis. Es sei $\rho(x) = k$. Also existiert $y \ge k$ und es gibt k Primzahlen $p + b_i$ (mit $b_0 = 0$) derart, dass $y < p < p + b_1 < \cdots < p + b_{k-1} \le y + x$. Dann ist $b_{k-1} < x$. Wenn es eine Primzahl $q \le k$ gäbe, so dass $\{b_i \bmod q \mid i = 0, 1, \ldots, k-1\}$ die Menge aller Kongruenzklassen modulo q wäre, dann gibt es i mit $-p \equiv b_i \pmod q$, daher wird $p + b_i$ von q geteilt und somit $q \le k \le y \le p + b_i = q$, was unmöglich ist. Daher ist $(b_1, b_2, \ldots, b_{k-1})$ zulässig und $k \le \rho^*(x)$. □

Es ist interessant, $\rho^*(x)$ mit $\pi(x)$ zu vergleichen. Numerische Berechnungen wurden erstmals von Schinzel (1961) durchgeführt; Selfridge (unveröffentlicht) wies nach, dass $\rho^*(x) \le \pi(x)$ für alle $x \le 500$ gilt. Der folgende Satz von Hensley & Richards (1974) zeigt, dass sich diese Situation letztendlich umkehrt:

Für jedes ε mit $0 < \varepsilon < \log 2$ gibt es ein $x_0 > 1$ derart, dass wenn $x \ge x_0$, dann

$$\rho^*(x) - \pi(x) > (\log 2 - \varepsilon)\frac{x}{(\log x)^2}.$$

Insbesondere $\lim\limits_{x\to\infty} \big(\rho^*(x) - \pi(x)\big) = \infty$.

Mit Hilfe eines gut durchdachten Computerprogramms von W. Stenberg wurde 1974 gezeigt, dass $\rho^*(20000) > \pi(20000)$. Es ist ein schwieriges Problem, die Größenordnung von $\rho^*(x)$ zu bestimmen. Stimmt es, dass $\rho^*(x) \sim \pi(x)$?

Aus der folgenden Vermutung geht insbesondere die Existenz von Primzahlmehrlingen hervor:

Primzahlmehrlingsvermutung.[3] *Wenn $k \ge 2$ und $(b_1, b_2, \ldots, b_{k-1})$ ein zulässiges $(k-1)$-Tupel positiver Zahlen ist, dann gibt es unendlich*

[3] Anm. d. Übers.: Diese Vermutung ist im Englischen als *Prime k-Tuples Conjecture* bekannt.

viele Primzahlen p derart, dass $p, p+b_1, \ldots, p+b_{k-1}$ sämtlich prim sind.

Insbesondere gibt es, falls $(b_1, b_2, \ldots, b_{k-1})$ zulässig und dicht ist, unendlich viele Primzahlmehrlinge vom Typ $(b_1, b_2, \ldots, b_{k-1})$.

In Kapitel 6, Abschnitt I werde ich eine Vermutung von Dickson betrachten, die von Schinzel & Sierpiński (1958) eingehend studiert wurde und aussagt, dass lineare Polynome unter bestimmten Bedingungen simultan Primzahlwerte annehmen. Die Primzahlmehrlingsvermutung besagt, dass wenn $(b_1, b_2, \ldots, b_{k-1})$ zulässig ist, die Polynome $X, X+b_1, \ldots, X+b_{k-1}$ unendlich oft simultan Primzahlwerte annehmen.

Der Beweis der Primzahlmehrlingsvermutung kann nicht vor dem Beweis der Primzahlzwillingsvermutung geführt werden. Trotzdem gibt es viele, die fest an ihre Richtigkeit glauben, unter ihnen vor allem Erdös. Auf dieser Stufe der Unwissenheit ist die Entscheidung, ob man an die Vermutung glaubt oder nicht, rein gefühlsmäßig.

Argumente der Befürworter. Man ist sich weitgehend einig, dass die Primzahlzwillingsvermutung richtig ist. Warum sollte dann die Primzahlmehrlingsvermutung für $k > 2$ nicht richtig sein? Man hat das Gefühl, dass diese Probleme für jedes $k \geq 2$ den gleichen Schwierigkeitsgrad haben und die Methoden zum Beweis der Primzahlzwillingsvermutung auch zum Beweis der umfassenderen Primzahlmehrlingsvermutung dienen werden. Das „Haus der Primzahlen“ ist sehr einladend – in seiner unermesslichen Ausdehnung kann es Zwillinge, Drillinge, Vierlinge, ... und alle Arten legitimer Primzahlfamilien aufnehmen.

Argumente der Gegner. Was man nicht sehen oder anfassen kann, existiert nicht. Tatsächlich wird wohl niemand jemals einem zulässigen Primzahlmehrling der Ordnung $10^{10^{10}}$ begegnen. So etwas ist unglaublich und es gibt absolut keine die Primzahlmehrlingsvermutung unterstützenden Belege. Auf wissenschaftlichere Weise ausgedrückt, hier das schöne Resultat von Hensley & Richards:

Die Vermutung von Hardy & Littlewood (Abschnitt I, H) *und die Primzahlmehrlingsvermutung können nicht gleichzeitig wahr sein.*

Beweis. Ich unterstelle die Richtigkeit der Primzahlmehrlingsvermutung und zeige, dass $\rho^*(x) \leq \rho(x)$ und somit $\rho^*(x) = \rho(x)$ für alle $x > 1$.

Es sei $\rho^*(x) = k$, also existiert ein zulässiges $(k-1)$-Tupel $(b_1, b_2, \ldots, b_{k-1})$ mit $b_{k-1} < x$. Nach der Primzahlmehrlingsvermutung gibt es unendlich viele Primzahlen p derart, dass $p, p+b_1, \ldots, p+b_{k-1}$ Primzahlen sind; man beachte, dass sie die Ungleichung $p-1 < p < p+b_1 < \cdots < p+b_{k-1} \leq (p-1)+x$ erfüllen. Daher gilt nach Definition von $\rho(x)$, $\rho(x) \geq k = \rho^*(x)$. Nach oben erwähntem Satz gibt es x_0 mit $\rho^*(x) > \pi(x)$ für alle $x \geq x_0$. Also hat die Ungleichung $\rho^*(x) \leq \rho(x)$ für jedes x zur Folge: Es gibt unendlich viele y derart, dass $\pi(x) < \rho(x) = \pi(x+y) - \pi(y)$. Und dies zeigt, dass die Vermutung von Hardy & Littlewood nicht wahr sein kann, wenn die Primzahlmehrlingsvermutung richtig ist. □

Eine Vermutung aus der Familie der Primzahlmehrlingsvermutung, die sich auf die Translation von Folgen bezieht, wurde von Golomb (1992) als offenes Problem formuliert:

Golombs Vermutung. *Es gibt eine wachsende Folge positiver Zahlen* $1 \leq a_1 < a_2 < \ldots$ *und eine ganze Zahl* $B \geq 1$ *derart, dass für jedes* $n \in \mathbb{Z}$ *die Anzahl der Primzahlen in der Folge* $a_1 + n < a_2 + n < \ldots$ *höchstens gleich* B *ist.*

Für den Fall, dass eine Schranke B nicht explizit gefordert ist, gibt es ein interessantes Beispiel: Für jedes $n \in \mathbb{Z}$ gibt es nur endlich viele Primzahlen der Form $((2k)!)^3 + n$. Dies ist für $n = 0$ oder $|n| \geq 2$ trivial. Ansonsten: $((2k)!)^3 - 1 = \big[(2k)! - 1\big]\big[(2k)!^2 + (2k)! + 1\big]$ und $((2k)!)^3 + 1 = \big[(2k)! + 1\big]\big[(2k)!^2 - (2k)! + 1\big]$. Aber natürlich gibt es für diese Folge keine Schranke B wie in der Vermutung.

Ford fand 1995 einen eleganten Beweis des folgenden Satzes:

Die Primzahlmehrlingsvermutung und Golombs Vermutung können nicht gleichzeitig wahr sein.

Beweis. Angenommen, mit der Folge $A = (a_i)_{i \geq 1}$ und $B \geq 1$ ist die Bedingung in Golombs Vermutung erfüllt. Bekanntlich gibt es eine Konstante $c > 0$, so dass für jedes $l \geq 2$,

$$\prod_{p \leq l} \left(1 - \frac{1}{p}\right) > \frac{c}{\log l}\,.$$

Es sei l derart, dass $cl/(\log l) > B$. Nun sei $A_l = \{a_1, a_2, \ldots, a_l\}$ und $E_2 = A_l \setminus (A_l \cap C)$, wobei C eine Kongruenzklasse von $\mathbb{Z}$ modulo 2 mit minimalem $\#(A_l \cap C)$ ist. Dann gilt $\#(A_l \cap C) \leq l/2$, somit

$\#(E_2) \geq l(1-1/2)$. Nach Definition gehört kein Element von E_2 zur Kongruenzklasse C modulo 2.

Es sei $E_3 = E_2 \smallsetminus (E_2 \cap C')$, wobei C' eine Kongruenzklasse von $\mathbb{Z}$ modulo 3 mit minimalem $\#(E_2 \cap C')$ ist; dann ist $\#(E_2 \cap C') \leq \#(E_2)/3$ und

$$\#(E_3) \geq \#(E_2)\left(1-\frac{1}{3}\right) \geq l\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right).$$

Man beachte, dass kein Element von E_3 zur Kongruenzklasse C' modulo 3 gehört.

Dieses Argument wiederholt man für alle Primzahlen $p \leq l$ und landet schließlich bei einer Menge E^*, wobei

$$\#(E^*) \geq l \prod_{p \leq l}\left(1-\frac{1}{p}\right) > \frac{cl}{\log l} > B.$$

Nach Definition gilt $\#(E^*) < l$ und für jede Primzahl $q \leq \#(E^*) < l$ ist die Menge der Kongruenzklassen $\{b \bmod q \mid b \in E^*\}$ echt in der Menge aller Kongruenzklassen modulo q enthalten. Dieses E^* ist eine zulässige Menge. Nach der Primzahlmehrlingsvermutung gibt es unendlich viele Primzahlen p derart, dass p und alle $p+b$ (mit $b \in E^*$) Primzahlen sind. Für jede solche Primzahl p enthält die Menge $\{a_i + p \mid i \geq 1\}$ mehr als B Primzahlen – was ein Widerspruch ist. □

Die folgende Konsequenz aus der Primzahlmehrlingsvermutung für Polynome $X^2 + X + c$ teilte A. Granville in einem Brief von 1989 mit (siehe Mollin, 1997). Es sei $f(X) = aX^2 + bX + c$ mit $a \geq b$. Angenommen, $a + b$ ist gerade. Wenn q eine ungerade Primzahl ist, die a teilt, dann teilt q auch b. Unter der Annahme der Richtigkeit der Primzahlmehrlingsvermutung gibt es für jedes $M > 1$ unendlich viele $n \geq 1$, so dass $f(0)+n$, $f(1)+n$, …, $f(M)+n$ Primzahlen sind. In der Terminologie von Kapitel 3, Abschnitt III, C, haben die verschobenen Polynome $g_n(X) = f(X) + n$ eine primzahlerzeugende Länge größer als M.

Beweis. Es sei $S = \{f(0), f(1), \ldots, f(M)\}$. Ich werde zeigen, dass S eine zulässige Menge ist. In der Tat gilt $f(0) \equiv f(1) \equiv \cdots \equiv f(M) \equiv c \pmod 2$. Wenn q eine ungerade Primzahl ist und $q \mid a$, dann auch $q \mid b$ und wieder $f(0) \equiv f(1) \equiv \cdots \equiv f(M) \equiv c \pmod q$. Nun sei $q \neq 2$ und q kein Faktor von a sowie u, a' dergestalt, dass $2u \equiv 1 \pmod q$ und $aa' \equiv 1 \pmod q$ gilt. Für jedes s,

$$as^2 + bs + c \equiv a(s^2 + a'bs) + c \equiv a(s + ua'b)^2 + (c - a'u^2b^2).$$

Die Menge der Restklassen $at^2 \pmod q$ enthält $(q+1)/2$ Elemente. Also existiert y derart, dass $y \not\equiv at^2 \pmod q$ für alle t. Es sei $z = y + (c - a'u^2b^2)$. Wenn es ein s mit $0 \le s \le M$ gibt, das $z \equiv f(s) \pmod q$ erfüllt, dann gilt

$$y + (c - a'u^2b^2) \equiv a(s + ua'b)^2 + (c - a'u^2b^2).$$

Daraus folgt, dass $y \equiv a(s + ua'b)^2 \pmod q$, was ein Widerspruch ist. Also ist die Menge S zulässig und nach der Primzahlmehrlingsvermutung gibt es unendlich viele n, so dass $g_n(X) = f(X) + n$ an den Stellen $s = 0, 1, \ldots, M$ Primzahlwerte annimmt. □

V Primzahlen in arithmetischer Folge

A Es gibt unendlich viele!

Einen klassischen Satz von großer Bedeutung bewies Dirichlet im Jahre 1837. Er besagt:

Wenn $d \ge 2$ und $a \ne 0$ ganze, teilerfremde Zahlen sind, dann enthält die arithmetische Folge

$$a, \quad a + d, \quad a + 2d, \quad a + 3d, \quad \ldots$$

unendlich viele Primzahlen.

Viele Spezialfälle dieses Satzes waren bereits bekannt gewesen, unter ihnen natürlich auch der Satz von Euklid (wenn $a = 1$, $d = 2$). Tatsächlich verläuft der Beweis der Fälle $d = 4$ oder $d = 6$ und $a = -1$ analog zu Euklids Beweis.

Unter Ausnutzung elementarer Eigenschaften quadratischer Reste lässt sich auch einfach zeigen, dass jede der folgenden arithmetischen Folgen unendlich viele Primzahlen enthält:

$d = 4$, $a = 1$;
$d = 6$, $a = 1$;
$d = 3$, $a = 1$;
$d = 8$, $a = 3$ oder $a = 5$ oder $a = 7$
(dies beinhaltet die Folgen mit $d = 4$);
$d = 12$, $a = 5$ oder $a = 7$ oder $a = 11$
(dies beinhaltet die Folgen mit $d = 6$).

Als Zutaten für einen einfachen Beweis der Fälle $d = 8, 16, \ldots$ oder allgemeiner $d = 2^r$ und $a = 1$ verwende man $f(N)$, wobei

$$f(X) = X^{2^{r-1}} + 1, \quad N = 2p_1p_2 \cdots p_n,$$

und die p_i sämtlich Primzahlen mit $p_i \equiv 1 \pmod{2^r}$ sind, und benutze dann den kleinen Satz von Fermat. Diese Hinweise sind für diejenigen Leser gedacht, die den Beweis selbst finden wollen.

Der Beweis für beliebiges d und $a = 1$ oder $a = -1$ ist ebenso elementar, wenn auch nicht einfach, und erfordert Kreisteilungspolynome und einige ihrer elementaren Eigenschaften.

Eine detaillierte Diskussion des Dirichletschen Satzes und verschiedener Beweisvarianten befindet sich in Hasses Buch *Vorlesungen über Zahlentheorie*.

Im Jahre 1949 fand Selberg analog zu seinem Beweis des Primzahlsatzes auch einen elementaren Beweis des Satzes von Dirichlet.

In Bezug auf Dirichlets Satz bewies de la Vallée Poussin das folgende Resultat zur Dichte von Primzahlen in Folgen. Für a, d wie zuvor und $x \geq 1$ sei

$$\pi_{d,a}(x) = \#\{p \text{ prim} \mid p \leq x,\ p \equiv a \pmod{d}\}.$$

Dann gilt

$$\pi_{d,a}(x) \sim \frac{1}{\varphi(d)} \cdot \frac{x}{\log x}\,.$$

Man beachte, dass die rechte Seite für alle a mit $\mathrm{ggT}(a, d) = 1$ gleich ist. Es folgt, dass

$$\lim_{x\to\infty} \frac{\pi_{d,a}(x)}{\pi(x)} = \frac{1}{\varphi(d)}\,,$$

was sich auch so ausdrücken lässt, dass die Menge der Primzahlen in der arithmetischen Folge $\{a+kd \mid k \geq 1\}$ eine natürliche Dichte $1/\varphi(d)$ hat (in Bezug auf die Menge aller Primzahlen).

Ungeachtet der Tatsache, dass das asymptotische Verhalten von $\pi_{d,a}(x)$ für jedes a mit $1 \leq a < d$ und $\mathrm{ggT}(a, d) = 1$ dasselbe ist, hatte Tschebyscheff bereits 1853 bemerkt, dass $\pi_{3,1}(x) < \pi_{3,2}(x)$ und $\pi_{4,1}(x) < \pi_{4,3}(x)$ für kleine x-Werte gilt; mit anderen Worten, es gibt bis x mehr Primzahlen der Form $3k + 2$ als solche der Form $3k + 1$ und mehr Primzahlen $4k + 3$ als $4k + 1$ (für nicht zu großes x). Gelten diese Ungleichungen für alle x? Die Situation ist in gewissem Sinne ähnlich der für die Ungleichung $\pi(x) < \mathrm{Li}(x)$. Wieder lässt sich analog zu Littlewoods Satz zeigen, dass die Ungleichungen unendlich oft

die Richtung wechseln. So berechnete Leech 1957, dass $x_1 = 26861$ die kleinste Primzahl ist, für die $\pi_{4,1}(x) > \pi_{4,3}(x)$; siehe auch Bays & Hudson (1978), die herausfanden, dass $x_1 = 608\,981\,813\,029$ die kleinste Primzahl ist, für die $\pi_{3,1}(x) > \pi_{3,2}(x)$ gilt.

Hudson leitete 1977 eine Formel ähnlich der von Meissel für $\pi(x)$ her, um $\pi_{d,a}(x)$ zu berechnen, was die genaue Anzahl der Primzahlen $p < x$ in der arithmetischen Folge $\{a + kd \mid k \geq 0\}$ angibt. Im selben Jahr wandten sich Hudson & Brauer einem detaillierten Studium der speziellen arithmetischen Folgen $4k \pm 1$, $6k \pm 1$ zu.

Ein erst in jüngerer Zeit bewiesener Satz beschäftigt sich mit aufeinander folgenden Primzahlen in arithmetischen Folgen. Es bezeichne $(p_n)_{n\geq 1}$ die ansteigende Folge aller Primzahlen. In seiner Dissertation bewies Shiu (1996) unter Verwendung ausgeklügelter analytischer Methoden (siehe auch seinen Artikel aus dem Jahr 2000):

Es seien a und d teilerfremde natürliche Zahlen mit $1 \leq a < d$. Dann gibt es positive reelle Zahlen x_0 und C (die von a und d abhängen) mit der folgenden Eigenschaft: Für jede reelle Zahl $x > x_0$ gibt es $n \geq 1$ und

$$k \geq C \left[\frac{\log_2 x \, \log_4 x}{(\log_3 x)^2} \right]^{1/\varphi(d)}$$

so dass $p_{n+k} \leq x$ und $p_{n+1} \equiv p_{n+2} \equiv \cdots \equiv p_{n+k} \equiv a \pmod{d}$.

Jede erlaubte arithmetische Folge enthält also beliebig lange Reihen aufeinander folgender Primzahlen. Der Grund ist der, dass mit wachsendem x auch k gegen Unendlich läuft. Es ist jedoch nicht sichergestellt, dass diese aufeinander folgenden Primzahlen selbst in arithmetischer Folge liegen.

B Die kleinste Primzahl in einer arithmetischen Folge

Mit $d \geq 2$ und dazu teilerfremdem $a \geq 1$ sei $p(d, a)$ die kleinste Primzahl in der arithmetischen Folge $\{a + kd \mid k \geq 0\}$. Ist es möglich, eine obere Schranke für $p(d, a)$ zu finden, die nur von a, d abhängt?

Es sei $p(d) = \max\{p(d, a) \mid 1 \leq a < d, \, \mathrm{ggT}(a, d) = 1\}$. Wiederum die Frage: Kann man eine obere, nur von d abhängige Schranke für $p(d)$ angeben? Was lässt sich über untere Schranken sagen?

Der Satz von Linnik von 1944, der eines der tiefsten Resultate der analytischen Zahlentheorie darstellt, sagt aus:

Es gibt $d_0 \geq 2$ und $L > 1$ derart, dass $p(d) < d^L$ für jedes $d \geq d_0$.

Man beachte, dass die absolute Konstante L, bezeichnet als *Linniks Konstante*, effektiv berechenbar ist.

Und es ist natürlich wichtig, den Wert von L zu berechnen. Pan (Cheng-Dong) war der Erste, der Linniks Konstante 1957 durch $L \leq 5448$ abschätzte. In der Folgezeit erschienen zahlreiche Artikel, in denen die Abschätzung für die Konstante verbessert wurde.

Rekord

Heath-Brown (1992) gelang es, die Abschätzung $L \leq 13{,}5$ von Chen & Liu (1989) durch $L \leq 5{,}5$ zu ersetzen. Frühere Rekorde stammten von Chen (1965), Jutila (1977) und Graham (1981).

Schinzel & Sierpiński (1958) und Kanold (1963) vermuteten, dass $L = 2$, das heißt, $p(d) < d^2$ für jedes genügend große $d \geq 2$. Präzise ausgedrückt bedeutet dies, dass sich für $1 \leq a < d$, $\mathrm{ggT}(a, d) = 1$ unter den Zahlen a, $a+d$, $a+2d, \ldots, a+(d-1)d$ immer eine Primzahl befindet.

Heath-Brown unterbreitete 1978 die Vermutung $p(d) \leq Cd(\log d)^2$, und 1979 stützte Wagstaff seinen Ansatz $p(d) \sim \varphi(d)(\log d)^2$ auf heuristische Betrachtungen.

In Bezug auf untere Schranken für $p(d)$ sei zunächst das folgende Resultat von Schatunowsky (1893) erwähnt, das unabhängig auch von Wolfskehl[4] 1901 erzielt wurde.

$d = 30$ ist die größte Zahl mit der folgenden Eigenschaft: Falls $1 \leq a < d$ und $\mathrm{ggT}(a, d) = 1$, dann ist $a = 1$ oder a ist eine Primzahl.

Der Beweis ist elementar und findet sich zum Beispiel in Landaus Buch *Primzahlen* (1909) auf Seite 229. Es folgt unmittelbar, dass $p(d) > d + 1$, wenn $d > 30$.

Schon der Primzahlsatz hat zur Folge, dass für jedes $\varepsilon > 0$ und genügend großes d gilt:

$$p(d) > (1 - \varepsilon)\varphi(d) \log d.$$

[4]Paul Wolfskehl kennt man gewöhnlich als den reichen Mathematiker, der einen beträchtlichen Preis für die Entdeckung eines Beweises von Fermats letztem Satz ausgesetzt hatte. Ich erzähle die Geschichte in meinem Buch *13 Lectures on Fermats Last Theorem*. An dieser Stelle möchte ich an ihn erinnern, stellvertretend für all die jungen Assistenten, die sich in den 90 Jahren nach der Preisauslobung daran erfreuen durften, in einem schier unendlichen Fluss von „Beweisen“ von Fermats letztem Satz Fehler zu finden. Der Satz wurde schließlich 1997 von Andrew Wiles bewiesen und er war es, dem der Preis zuerkannt wurde.

Daraus ergibt sich, dass

$$\liminf \frac{p(d)}{\varphi(d)\log d} \geq 1.$$

Im Jahre 1980 bewies Pomerance das schärfere Resultat

$$\liminf \frac{p(d)}{\varphi(d)\log d} \geq e^{\gamma} = 1{,}78107\ldots$$

(wobei γ Eulers Konstante ist). Sei andererseits Q die Menge aller Zahlen $d \geq 2$ mit mehr als $\exp(\log_2 d/\log_3 d)$ verschiedenen Primfaktoren. Dann gilt für jedes d außerhalb der Menge Q,

$$\liminf \frac{p(d)}{\varphi(d)\log d} \times t_d \geq e^{\gamma},$$

wobei

$$t_d = \frac{(\log_3 d)^2}{(\log_2 d)(\log_4 d)}\,;$$

man beachte, dass $\lim_{d\to\infty} t_d = 0$. Insbesondere ist die Menge der Zahlen $p(d)/\big(\varphi(d)\log d\big)$ unbeschränkt.

In diesem Zusammenhang sei angemerkt, dass Prachar und Schinzel 1961 und 1962 einige Ergebnisse bezüglich dieser Frage erzielt hatten.

Es sollte nicht unerwähnt bleiben, dass die Menge Q die Dichte Null hat, da die Anzahl verschiedener Primfaktoren von d durchschnittlich gleich $\log_2 d$ ist.

Granville & Pomerance vermuteten 1990, dass

$$p(d) \geq C\varphi(d)(\log d)^2$$

für $d \geq 2$ und eine Konstante $C > 0$.

C Primzahlreihen in arithmetischer Folge

Ich betrachte nun die Frage nach der Existenz von Reihen von k Primzahlen $p_1 < p_2 < p_3 < \cdots < p_k$ mit Differenz $p_2 - p_1 = p_3 - p_2 = \cdots = p_k - p_{k-1}$, das heißt, diese Primzahlen befinden sich in arithmetischer Folge.

Im Jahre 1939 bewies van der Corput, dass es unendlich viele Reihen mit drei Primzahlen in arithmetischer Folge gibt (siehe Abschnitt VI); dies wurde 1944 erneut von Chowla gezeigt und nochmal von Heath-Brown 1985 als Korollar eines allgemeineren Satzes.

Obwohl es einfach ist, Beispiele mit vier (oder gar mehr) Primzahlen in arithmetischer Folge zu finden, bleibt die Frage: Gibt es für jedes $k \geq 4$ unendlich viele arithmetische Folgen, die k Primzahlen enthalten?

Für $k = 4$ zeigte Heath-Brown 1981, dass es unendlich viele arithmetische Folgen gibt, die vier Zahlen enthalten, von denen drei Primzahlen sind und die vierte ein Produkt von zwei nicht notwendigerweise verschiedenen Primfaktoren.

Bis vor kurzem war nicht einmal die schwächere Vermutung bewiesen, dass es für jedes $k \geq 4$ wenigstens eine arithmetische Folge aus k Primzahlen gibt. Dies ist nun B. Green & T. Tao (2004, veröffentlicht 2008) mit Hilfe einer sehr originellen und schwierigen Methode gelungen. Sie bewiesen den Satz:

Für jedes $k \geq 4$ existiert mindestens eine arithmetische Folge aus k natürlichen Zahlen, die alle Primzahlen sind.

Diese Arbeit hat Tao auf dem Internationalen Mathematikerkongress 2006 in Madrid die Fields-Medaille eingebracht. Ein wichtiger Bestandteil des Beweises ist neben einigen sehr innovativen Argumenten ein inzwischen klassischer Satz von Szemerédi, den ich nun formulieren möchte.

Es sei A eine Menge natürlicher Zahlen. Für jedes $n \geq 1$ bezeichne $A(n)$ die Menge aller Elemente a von A mit $a \leq n$. Man sagt, die Menge A hat die Dichte δ, wenn $\lim_{n\to\infty} \#A(n)/n$ existiert und gleich δ ist. Der Satz von Szemerédi besagt, dass wenn die Menge A eine positive Dichte hat, dann enthält A für jedes $k \geq 3$ unendlich viele arithmetische Folgen der Länge k.

Der Beweis von Green und Tao ist nicht konstruktiv, liefert also keine Beispiele. Es wurden jedoch intensive Computersuchen nach langen Primzahlreihen in arithmetischer Folge durchgeführt.

Rekord

Im April 2010 entdeckten P. Perichon, J. Wróblewski und G. Reynolds im Rahmen von PrimeGrid die erste Reihe mit 26 Primzahlen in arithmetischer Folge. Sie beginnt mit $p = 43\,142\,746\,595\,714\,191$, und die Differenz beträgt $d = 5\,283\,234\,035\,979\,900$.

Die vorherigen Rekorde mit der entsprechenden Anzahl von Folgengliedern wurden wie folgt aufgestellt:

1977: 17 Glieder durch S. Weintraub,

1982: 18 Glieder durch P. Pritchard,

1985: 19 Glieder durch P. Pritchard,

1987: 20 Glieder durch J. Young und J. Fry,

1993: 22 Glieder durch das Gemeinschaftsprojekt Pritchard,

2004: 23 Glieder durch M. Frind, P. Jobling und P. Underwood,

2006: 24 Glieder durch J. Wróblewski,

2008: 25 Glieder durch R. Chermoni und J. Wróblewski.

In die von P. Pritchard (Griffith University in Queensland, Australien) koordinierte Suche waren mehr als 60 Computer einbezogen. Es handelte sich um ein wahrlich internationales Projekt: Die 22-teilige Reihe wurde in Bergen, Norwegen gefunden.

Im Zusammenhang mit dieser Fragestellung ist die folgende Aussage von M. Cantor (1861), zitiert in Dicksons *History of the Theory of Numbers*, Bd. I, S. 425, leicht zu beweisen:

Es sei $d \geq 2$ und a, $a+d, \ldots, a+(n-1)d$ seien n Primzahlen in arithmetischer Folge. Zudem sei q die größte Primzahl mit $q \leq n$. Dann gilt: $\prod_{p \leq q} p$ teilt d oder $a = q$ und $\prod_{p<q} p$ teilt d.

Beweis. Zunächst eine einfache Anmerkung. Wenn p eine Primzahl ist, die d nicht teilt und wenn a, $a+d, \ldots, a+(p-1)d$ Primzahlen sind, dann sind diese Zahlen paarweise inkongruent modulo p und p teilt genau eine von ihnen. Man nehme nun an, dass d von $\prod_{p \leq q} p$ nicht geteilt wird, das heißt es gibt eine Primzahl $p \leq n$, die d nicht teilt. Wähle das kleinste solche p. Nach der Anmerkung existiert j, $0 \leq j \leq p-1$, so dass p die Summe $a+jd$ teilt, also $p = a+jd$, da $a+jd$ prim ist. Aber a ist eine Primzahl; falls $a \neq a+jd$, dann wird d von a geteilt (nach Wahl von p), also ist a Teiler von p, das heißt $a = p+jd$. Dies beweist, dass $p = a$. Falls $p < q$, dann $p \leq n-1$, also ist p Teiler von $a+pd$, somit $p = a+pd = p(1+d)$, was unsinnig ist. Es ist daher gezeigt, dass wenn $\prod_{p \leq q} p$ die Zahl d nicht teilt, dann $q = a$ und $\prod_{p<q} p$ teilt d. □

Ein Spezialfall dieser Aussage wurde von Lagrange bewiesen.

An dieser Stelle möchte ich daran erinnern, dass ich mich in Kapitel 3, Abschnitt II bereits einer noch schwierigeren Frage zugewandt hatte, nämlich der Suche nach Reihen von p Primzahlen in arithmetischer Folge, deren kleinstes Glied p selbst ist.

Ein verwandtes und noch schwierigeres Problem ist das folgende. Gibt es beliebig lange arithmetische Folgen von *aufeinander folgenden* Primzahlen?

Rekord

Die längste bekannte Reihe aufeinander folgender Primzahlen in arithmetischer Folge umfasst 10 Glieder. Die erste Primzahl ist

$$p = 1009969724697142476377866555879698403295093246\text{-}\\ 8919004180360341775890434170334888215906722971 9,$$

die Differenz der Folge ist 210.

Diese Folge von Primzahlen wurde am 2. März 1998 von M. Toplic entdeckt, einer von über 100 internationalen Teilnehmern eines von H. Dubner, T. Forbes, N. Lygeros, M. Mizony und P. Zimmermann geleiteten Projekts. Schon zuvor war es am 24. Januar 1998 M. Toplic gewesen, der das „Glückslos“ gezogen hatte und 9 aufeinander folgende Primzahlen in arithmetischer Folge fand: Die Differenz war wiederum 210 und die kleinste Primzahl

$$p = 9967943206670108648449065369585356163898236408\text{-}\\ 0991618395774048585529071475461114799677694651.$$

VI Goldbachs berühmte Vermutung

Im Jahre 1742 äußerte Goldbach in einem Brief gegenüber Euler, dass er glaube:

(G) *Jede ganze Zahl $n > 5$ ist die Summe von drei Primzahlen.*

Euler erwiderte, dass sich daraus leicht die folgende, äquivalente Aussage ableiten lässt:

(G′) *Jede gerade Zahl $2n \geq 4$ ist die Summe zweier Primzahlen.*

Denn wenn man (G′) als wahr voraussetzt und wenn gilt $2n \geq 6$, dann ist $2n - 2 = p + p'$ und daher $2n = 2 + p + p'$, wobei p, p' Primzahlen sind. Außerdem folgt $2n + 1 = 3 + p + p'$, was (G) beweist.

Wenn man umgekehrt (G) als wahr annimmt und $2n \geq 4$ gilt, dann folgt $2n + 2 = p + p' + p''$ mit Primzahlen p, p', p''; und es ist notwendigerweise $p'' = 2$ (zum Beispiel) und $2n = p + p'$.

Man beachte, dass (G′) trivialerweise für unendlich viele gerade Zahlen wahr ist: $2p = p + p$ (für jede Primzahl).

Ein verwandtes, jedoch schwächeres Problem ist das folgende: Ist es richtig, dass jede ungerade Zahl größer als 5 die Summe dreier Primzahlen ist? Dies nennt man die *ungerade Goldbachsche Vermutung*. Sie würde zur Folge haben, dass jede Zahl größer als 6 die Summe von höchstens vier Primzahlen ist.

In der Zeit vor der Entwicklung der Siebtheorie und verfeinerter analytischer Methoden kam man in Bezug auf diese Vermutungen praktisch nicht weiter. Und trotz aller Versuche sind die Probleme immer noch ungelöst.

In der Vergangenheit verfolgte man im Wesentlichen drei Ansätze, die man, wenn auch möglicherweise etwas unzureichend, mit den Schlüsselwörtern „asymptotisch“, „Fastprimzahl“ und „Basis“ umschreiben könnte.

(A) Eine asymptotische Aussage ist eine, die für alle genügend großen Zahlen gilt.

Das erste wichtige Resultat geht auf Hardy & Littlewood und das Jahr 1923 zurück – es handelt sich um einen asymptotischen Satz. Mit Hilfe der Kreismethode und einer modifizierten Form der Riemannschen Vermutung konnten sie zeigen, dass es ein n_0 derart gibt, dass jede ungerade Zahl $n \geq n_0$ die Summe dreier Primzahlen ist.

Im Jahre 1937 fand Winogradoff einen Beweis des Satzes von Hardy & Littlewood, der nicht auf die Riemannsche Vermutung zurückgreift. Heath-Brown gab 1985 einen anderen Beweis dieses Satzes an, ohne explizite Angabe eines Wertes für n_0.

Bei genauerer Prüfung des Beweises von Winogradoff gelang es Borodzkin 1956 zu zeigen, dass man $n_0 = 3^{3^{15}} \approx 10^{7000000}$ verwenden kann. Weitere Verbesserungen stammen von Chen & Wang, die 1989 die Schranke $n_0 = 10^{43000}$ ermittelten und dies 1996 auf $n_0 = 10^{7194}$ senken konnten. Dieser Wert ist allerdings immer noch zu groß, um den fehlenden Bereich kleiner ungerader Zahlen durch Computerverifikation abzudecken.

Im Jahre 1997 lösten Deshouillers, Effinger, te Riele & Zinoviev das Problem der drei Primzahlen für jede ungerade Zahl größer als 5, allerdings unter Voraussetzung einer Vermutung ähnlich der Riemannschen.

(B) Es sei $k \geq 1$ und $r \leq k$. Eine natürliche Zahl der Form $p_1 p_2 \cdots p_r$, wobei $p_1, p_2, \ldots, p_r$ Primzahlen sind (nicht notwendigerweise verschieden), heißt eine *k-Fastprimzahl*. Die Menge aller k-Fastprimzahlen wird mit P_k bezeichnet.

Der Ansatz über die Fastprimzahlen besteht darin zu zeigen, dass es $h, k \geq 1$ derart gibt, dass jede genügend große gerade Zahl die Summe einer k-Fastprimzahl und einer h-Fastprimzahl ist. Dabei ist natürlich beabsichtigt zu zeigen, dass man sowohl für h als auch k die Zahl 1 wählen kann.

Das erste Resultat in dieser Richtung gelang Brun (1919, *C.R. Acad. Sci. Paris*): Jede genügend große gerade Zahl ist die Summe zweier 9-Fastprimzahlen.

Durch Einsatz komplizierterer Siebtypen wurden viele Fortschritte erzielt. Selberg zeigte 1950, dass jede genügend große gerade Zahl in der Menge $P_2 + P_3$ der Summen von Zahlen aus P_2 und P_3 enthalten ist.

Im Gegensatz zu diesen Resultaten, die zwei zerlegbare Summanden beinhalten, konnte Rényi 1947 beweisen, dass es eine Zahl $k \geq 1$ derart gibt, dass jede genügend große gerade Zahl in $P_1 + P_k$ liegt. In weiteren Arbeiten wurden explizite Werte für k angegeben.

Das bis heute beste Resultat – und eines, das dem Beweis der Goldbachschen Vermutung am Nächsten kommt – stammt von Chen (Ankündigung der Resultate 1966; detaillierte Beweise 1973, 1978). In seinem berühmten Artikel bewies Chen:

Jede genügend große gerade Zahl lässt sich in der Form $2n = p + m$ darstellen, wobei p eine Primzahl ist und $m \in P_2$.

Zur selben Zeit bewies Chen das „konjugierte“ Resultat: Es gibt unendlich viele Primzahlen p derart, dass $p + 2 \in P_2$; dies kommt dem Beweis der Unendlichkeit der Anzahl der Primzahlzwillinge sehr nahe.

Dieselbe Methode eignet sich auch für den Nachweis, dass es für jede gerade Zahl $2k \geq 2$ unendlich viele Primzahlen p mit der Eigenschaft gibt, dass $p + 2k \in P_2$; also ist $2k$ in unendlich vielen Fällen gleich der Differenz $m - p$ ($m \in P_2$, p prim).

Ein Beweis von Chens Satz findet sich im Buch von Halberstam & Richert. Siehe auch den einfacheren Beweis von Ross (1975).

(C) Der „Basis“-Ansatz begann mit dem berühmten Satz von Schnirelmann (1930), dessen Beweis zum Beispiel in den Büchern von Landau (1937) und Gelfond & Linnik (1965 ins Englische übersetzt) zu finden ist:

Es gibt eine positive ganze Zahl S derart, dass jede genügend große Zahl Summe von höchstens S Primzahlen ist.

Es folgt, dass es eine positive Zahl $S_0 \geq S$ mit der Eigenschaft gibt, dass jede Zahl (größer als 1) Summe von höchstens S_0 Primzahlen ist. S_0 nennt man die *Schnirelmann-Konstante*. Goldbachs Vermutung kann man dadurch ausdrücken, dass $S_0 = 3$.

In seinem netten, kleinen Buch von 1947 schrieb Khinchin ein interessantes und leicht zugängliches Kapitel über Schnirelmanns Ideen zu den Basen und zur Dichte von Zahlenfolgen.

Schnirelmanns Konstante S_0 wurde in zahlreichen Berechnungen effektiv abgeschätzt.

Rekord

Die bis heute beste Abschätzung für Schnirelmanns Konstante fand Ramaré 1995: $S_0 \leq 6$. Die bis dahin beste Abschätzung $S_0 \leq 19$ stammte von Riesel & Vaughan (1983).

Richert bewies 1949 das folgende Analogon zu Schnirelmanns Satz: Jede Zahl $n > 6$ ist die Summe verschiedener Primzahlen.

An dieser Stelle sei bemerkt, dass Schinzel 1959 zeigte, dass Goldbachs Vermutung die folgende Aussage impliziert (und damit äquivalent zu ihr ist): Jede Zahl $n > 17$ ist die Summe von genau drei verschiedenen Primzahlen. Also wird Richerts Resultat als Korollar aus der Vermutung von Goldbach folgen (falls und wenn diese als richtig nachgewiesen wird).

(D) Die Anzahl der Darstellungen

Ich möchte mich nun der Anzahl $r_2(2n)$ der Darstellungen von $2n \geq 4$ als Summe zweier Primzahlen zuwenden. *A priori* kann $r_2(2n)$ sogar null sein (solange Goldbachs Vermutung nicht bewiesen ist).

Hardy & Littlewood fanden 1923 die folgende asymptotische Formel, die zunächst auf einer modifizierten Form der Riemannschen Vermutung beruhte; spätere Arbeiten von Winogradoff beseitigten diese Abhängigkeit:

$$r_2(2n) \leq C \frac{2n}{(\log 2n)^2} \log\log 2n.$$

Für $n > 2$ sei $\pi^*(n)$ die Anzahl der Primzahlen p mit $n/2 \leq p \leq n-2$. Sicher ist $r_2(n) \leq \pi^*(n)$. Deshouillers, Granville, Narkiewicz & Pomerance bewiesen 1993, dass $n = 210$ die größte Zahl ist, für die $r_2(n) = \pi^*(n)$ gilt.

Powell fragte 1985 nach einem elementaren Beweis der folgenden Tatsache (als Aufgabe im *Mathematics Magazine*): Für jedes $k > 0$

gibt es unendlich viele gerade Zahlen $2n$ derart, dass $r_2(2n) > k$. Eine Lösung von Finn & Frohliger wurde 1986 veröffentlicht.

Hier mein eigener Beweis, der nur die Kenntnis voraussetzt, dass es mindestens $x/(2\log x)$ Primzahlen $p \le x$ gibt, also eine abgeschwächte Version von Tschebyscheffs Ungleichung.

Beweis. Es sei x derart, dass $x/(2\log x) > \sqrt{2kx}+1$ und P eine Menge ungerader Primzahlen $p \le x$ mit mindestens $x/(2\log x)$ Elementen. Darüber hinaus sei P_2 die Menge von Paaren (p,q) mit $p < q$ und $p, q \in P$. Die Menge P_2 hat mindestens

$$\frac{1}{2} \cdot \frac{x}{2\log x}\left(\frac{x}{2\log x} - 1\right)$$

Elemente. Nun sei $f(p,q) = p+q$, so dass das Bild von f in der Menge gerader Zahlen kleiner gleich $2x-2$ enthalten ist; das Bild hat also höchstens $x-4$ Elemente. Das heißt, es gibt $n \le 2x-2$ derart, dass die Menge von Paaren $(p,q) \in P_2$ mit $p+q=n$ mindestens

$$\frac{P_2}{x-4} > \frac{1}{2x}\left(\frac{x}{2\log x} - 1\right)^2 > k$$

Elemente hat. □

(E) Die Menge der Ausnahmen.

Für jedes $x \ge 4$ sei

$$G'(x) = \#\{2n \mid 2n \le x, 2n \text{ ist nicht Summe zweier Primzahlen}\}.$$

Van der Corput (1937), Estermann (1938) und Tschudakoff (1938) bewiesen unabhängig voneinander, dass $\lim G'(x)/x = 0$ und sogar $G'(x) = O(x/(\log x)^\alpha)$ für jedes $\alpha > 0$. Ein weiterer Beweis stammt von Heath-Brown aus dem Jahre 1985.

Das in dieser Richtung beste Resultat ist Gegenstand einer tiefschürfenden Arbeit von Montgomery & Vaughan (1975) und besagt: Es gibt eine effektiv berechenbare Konstante α mit $0 < \alpha < 1$ derart, dass für jedes genügend große x gilt, dass $G'(x) < x^{1-\alpha}$. Chen & Pan zeigten 1980, dass $\alpha = 1/100$ eine mögliche Wahl ist. In einem zweiten Artikel (1983) erreichte Chen den Wert $\alpha = 1/25$ (unabhängig fand dies auch Pan).

Hier die Rekorde numerischer Berechnungen zur Goldbachschen Vermutung.

Rekorde

A. Zunächst das Problem der drei Primzahlen. Saouter verifizierte 1998, dass jede ungerade Zahl unterhalb von 10^{20} die Summe von höchstens drei Primzahlen ist.

B. Nun zum Problem von Goldbach. T. Oliveira e Silva bestätigte Goldbachs Vermutung für alle $p < 1{,}6 \times 10^{18}$. Diese Grenze erreichte er 2009, und er setzt seine Berechnungen weiter fort.

Die Grenzen der früheren Rekorde lauten wie folgt:

1965: 10^8 von Stein & Stein,

1989: 2×10^{10} von Granville, van de Lune & te Riele,

1993: 4×10^{11} von Sinisalo,

1998: 10^{14} von Deshouillers, te Riele & Saouter,

1998: 4×10^{14} von Richstein (veröffentlicht 2001),

2003: 2×10^{16} von Oliveira e Silva.

Eine Art Goldbach-Problem

Die Frage, der nun nachgegangen werden soll, ist, ob sich jede ungerade Zahl als Summe einer Primzahl und (natürlich keiner weiteren Primzahl, sondern) einer Zweierpotenz darstellen lässt. Das Problem ähnelt also sowohl der Goldbachschen Vermutung als auch der Primzahlzwillingsvermutung. Aufgebracht wurde es von Prinz A. de Polignac, der 1849 behauptete, dass jede ungerade natürliche Zahl Summe einer Primzahl und einer Zweierpotenz sei. Er stellte seinen Irrtum rasch fest, denn 959 abzüglich irgendeiner Zweierpotenz ergibt nie eine Primzahl. Siehe Dicksons *History of the Theory of Numbers*, Band I, Seite 424.

Es verbleibt das Studium der Menge $A = \{p+2^k \mid p \text{ ist eine ungerade Primzahl und } k \geq 1\}$. Ich gebe hier nur eine Übersicht der erzielten Resultate. Romanoff bewies 1934, dass A eine positive Dichte hat, das heißt, es gibt $C > 0$ mit $\#\{m \in A \mid m \leq x\}/x > C$ (für alle $x \geq 1$).

Erdös untersuchte das Problem im Jahre 1950. Aus dem Primzahlsatz folgt zunächst $\#\{m \in A \mid m \leq x\} = O(x)$. Er zeigte ferner, dass es eine arithmetische Folge aus ungeraden Zahlen gibt, die keine Zahl der Form $p + 2^k \in A$ enthält.

Die Zahlen $n = 7$, 15, 21, 45, 75, 105 haben die Eigenschaft, dass $n - 2^k$ für alle k mit $2^k < n$ prim ist. Erdös vermutete, dass dies die einzigen solchen Beispiele sind. Es sei $R(n) = \#\{(p, k) \mid p \text{ ist eine ungerade Primzahl, } k \geq 1 \text{ und } p + 2^k = n\}$. Erdös bewies die Existenz eines $C > 0$ derart, dass $R(n) > C \log\log n$ für unendlich viele n gilt.

VII Die Verteilung von Pseudoprimzahlen und Carmichael-Zahlen

Ich werde nun Ergebnisse über die Verteilung von Pseudoprimzahlen und von Carmichael-Zahlen vorstellen.

A Verteilung von Pseudoprimzahlen

Es sei $P\pi(x)$ die Anzahl der Pseudoprimzahlen (zur Basis 2) kleiner oder gleich x und $(\mathrm{psp})_1 < (\mathrm{psp})_2 < \cdots < (\mathrm{psp})_n < \cdots$ die wachsende Folge der Pseudoprimzahlen.

Erdös gab 1949 und 1950 die folgenden Abschätzungen an:

$$C \log x < P\pi(x) < \frac{x}{e^{\frac{1}{3}(\log x)^{1/4}}}$$

(für genügend großes x und $C > 0$). Unter Verwendung der in Kapitel 2, Abschnitt VIII vorgestellten Methode von Lehmer zur Generierung unendlich vieler Pseudoprimzahlen zur Basis 2 lässt sich darüber hinaus auf einfache Weise zeigen, dass für $x \geq 341$ gilt: $0{,}171 \log x \leq P\pi(x)$. Diese Abschätzungen wurden später deutlich verbessert, wie in Kürze zu sehen sein wird.

Es lässt sich nun leicht ableiten, dass

$$\sum_{n=1}^{\infty} \frac{1}{(\mathrm{psp})_n}$$

konvergent ist (erstmals von Szymiczek 1967 bewiesen), während

$$\sum_{n=1}^{\infty} \frac{1}{\log (\mathrm{psp})_n}$$

divergiert (zuerst von Mąkowski 1974 gezeigt).

Es wird sich als praktisch herausstellen, die folgenden Bezeichnungen für die Zählfunktionen der Pseudoprimzahlen sowie der Euler- und starken Pseudoprimzahlen zu beliebigen Basen $a \geq 2$ einzuführen:

$$\begin{aligned}
&P\pi_a(x) = \#\{n \mid 1 \leq n \leq x,\ n \text{ ist } \mathrm{psp}(a)\}, && P\pi(x) = P\pi_2(x),\\
&EP\pi_a(x) = \#\{n \mid 1 \leq n \leq x,\ n \text{ ist } \mathrm{epsp}(a)\}, && EP\pi(x) = EP\pi_2(x),\\
&SP\pi_a(x) = \#\{n \mid 1 \leq n \leq x,\ n \text{ ist } \mathrm{spsp}(a)\}, && SP\pi(x) = SP\pi_2(x).
\end{aligned}$$

Offensichtlich gilt $SP\pi_a(x) \leq EP\pi_a(x) \leq P\pi_a(x)$.

Ich betrachte nun Abschätzungen für obere und untere Schranken dieser Funktionen.

Pomerance verbesserte 1981 ein früheres Resultat von Erdös (1956) über die obere Schranke von $P\pi(x)$ und zeigte, dass für alle großen x,

$$P\pi(x) \leq \frac{x}{l(x)^{1/2}},$$

mit

$$l(x) = e^{\log x \log\log\log x / \log\log x}.$$

Dieselbe Schranke gilt auch für $P\pi_a(x)$ mit beliebiger Basis $a \geq 2$.

Bezüglich unterer Schranken stammt das beste Resultat bis heute ebenfalls von Pomerance 1982 (siehe Anmerkung 3 seines Artikels):

$$e^{(\log x)^\alpha} \leq SP\pi_a(x),$$

wobei $\alpha = 5/14$.

Tabellen mit Pseudoprimzahlen legen den Verdacht nahe, dass es für jedes $x \geq 170$ eine Pseudoprimzahl zwischen x und $2x$ gibt. Allerdings wurde dies noch nicht bewiesen. Dazu sei das folgende Resultat von Rotkiewicz (1965) erwähnt:

Wenn n eine ganze Zahl größer als 19 *ist, dann gibt es eine Pseudoprimzahl zwischen n und n^2. Darüber hinaus existiert für jedes $\varepsilon > 0$ ein $x_0 = x_0(\varepsilon) > 0$ derart, dass für $x > x_0$ immer eine Pseudoprimzahl zwischen x und $x^{1+\varepsilon}$ liegt.*

Im Zusammenhang mit Pseudoprimzahlen in arithmetischen Folgen bewies Rotkiewicz 1963 und 1967:

Wenn $a \geq 1$, $d \geq 1$ und $\mathrm{ggT}(a, d) = 1$*, dann gibt es unendlich viele Pseudoprimzahlen in der arithmetischen Folge $\{a + kd \mid k \geq 1\}$.*

Es bezeichne $\mathrm{psp}(d, a)$ die kleinste Pseudoprimzahl in dieser arithmetischen Folge. Rotkiewicz zeigte 1972:

Für jedes $\varepsilon > 0$ und jedes genügend große d gilt $\log \mathrm{psp}(d, a) < d^{4L^2+L+\varepsilon}$*, wobei L Linniks Konstante bezeichnet* (siehe Abschnitt IV).

Obige Ergebnisse wurden von van der Poorten & Rotkiewicz 1980 erweitert: Falls $a, d \geq 1$, $\mathrm{ggT}(a, d) = 1$, dann enthält die arithmetische Folge $\{a + kd \mid k \geq 1\}$ unendlich viele ungerade starke Pseudoprimzahlen zu jeder Basis $b \geq 2$.

B Verteilung von Carmichael-Zahlen

Ich werde mich nun der Verteilung der Carmichael-Zahlen zuwenden. Es bezeichne $CN(x)$ die Anzahl der Carmichael-Zahlen n mit $n \leq x$.

Zunächst die oberen Schranken für $CN(x)$. Erdös zeigte 1956, dass eine Konstante $\alpha > \frac{1}{2}$ existiert, so dass für jedes genügend große x

$$CN(x) \leq \frac{x}{l(x)^{\alpha}},$$

wobei $l(x)$ wie oben definiert ist.

Pomerance, Selfridge & Wagstaff verbesserten diese Abschätzung 1980 wie folgt. Für jedes $\varepsilon > 0$ gibt es $x_0(\varepsilon) > 0$ derart, dass für $x \geq x_0(\varepsilon)$ gilt:

$$CN(x) \leq \frac{x}{l(x)^{1-\varepsilon}}\,.$$

Das Problem, eine untere Schranke für $CN(x)$ zu finden, ist schwierig. Im Beweis von Alford, Granville & Pomerance (1994) wurde neben der Unendlichkeit der Anzahl der Carmichael-Zahlen auch gezeigt, dass $CN(x) \geq x^{2/7}$ für alle hinreichend großen x.

Es gibt gute Gründe dafür anzunehmen, dass $CN(x) \geq x/l(x)^{1-\varepsilon}$ (für genügend großes x), wie es von Pomerance, Selfridge & Wagstaff vermutet wurde. Eine gut verständliche Darstellung dieser Ergebnisse gab Granville 1992.

Ich berichte nun von Tabellen mit Pseudoprimzahlen und Carmichael-Zahlen. Poulet bestimmte 1938 alle (ungeraden) Pseudoprimzahlen (zur Basis 2) bis 10^8. Carmichael-Zahlen waren in Poulets Tabelle mit Sternchen versehen. Swift stellte 1975 eine Tabelle aller Carmichael-Zahlen bis 10^9 zusammen, und Yorinaga ging 1979 bis 10^{10}.

Die Tabelle von Pomerance, Selfridge & Wagstaff (1980) umfasst Pseudoprimzahlen, Euler-Pseudoprimzahlen, starke Pseudoprimzahlen (zur Basis 2) und Carmichael-Zahlen und reicht bis 25×10^9. Sie wurde von Pinch 1992 bis 10^{12} und 2000 bis 10^{13} ausgedehnt. In neuerer Zeit hat W.F. Galway alle Pseudoprimzahlen bis 10^{15} aufgelistet. In seiner Tabelle sind die spsp(2) und die Carmichael-Zahlen entsprechend markiert. Die epsp(2) wurden eigens für die folgende Tabelle ausgesondert und gezählt.

Tabelle 18. $P\pi(x), EP\pi(x), SP\pi(x)$ und $CN(x)$

x	$P\pi(x)$	$EP\pi(x)$	$SP\pi(x)$	$CN(x)$
10^3	3	1	0	1
10^4	22	12	5	7
10^5	78	36	16	16
10^6	245	114	46	43
10^7	750	375	162	105
10^8	2057	1071	488	255
10^9	5597	2939	1282	646
10^{10}	14884	7706	3291	1547
25×10^9	21853	11347	4842	2163
10^{11}	38975	20417	8607	3605
10^{12}	101629	53332	22407	8241
10^{13}	264239	139597	58892	19279
10^{14}	687007	364217	156251	44706
10^{15}	1801533	957111	419489	105212

Im August 2009 haben J. Feitsma von der Rijksuniversiteit Groningen und J. Gilchrist von der Carleton University in Ottawa unabhängig voneinander die folgenden Werte ermittelt:

$$P\pi(10^{16}) = 4\,744\,920, \quad P\pi(10^{17}) = 12\,604\,009.$$

Die Tabelle der Carmichael-Zahlen wurde 1990 von Jaeschke bis 10^{12} erweitert. Sie wurde von Pinch 1993 zunächst auf 10^{15} ausgedehnt (wobei geringfügige Ungenauigkeiten in Jaeschkes Tabelle korrigiert wurden). Pinch setzte seine Tabellierungsarbeit später fort und erreichte 10^{16} in 1998, 10^{17} in 2005, 10^{18} in 2006 und schließlich 10^{21} im Mai 2007. Tabelle 19 fasst seine Ergebnisse zusammen und zeigt die Anzahl der Carmichael-Zahlen bis 10^M, $3 \le M \le 21$, die jeweils k verschiedene Primfaktoren haben.

In diesem Zusammenhang erstellte Pinch weitere Tabellen, insbesondere folgenden Inhalts:

(1) Kleinste Carmichael-Zahl mit k Primfaktoren, für $3 \le k \le 35$.

(2) Anzahl der Carmichael-Zahlen in den Restklassen modulo 5, 7, 11, 12, bis 25×10^9, sowie bis 10^M für $11 \le M \le 18$.

(3) Häufigkeit, mit der jede Primzahl $p \leq 97$ überhaupt als Primfaktor (bzw. als kleinster Primfaktor) einer Carmichael-Zahl auftritt, jeweils bis zu den soeben genannten Grenzen.

Tabelle 19. Anzahl der Primfaktoren von Carmichael-Zahlen

	k										
M	3	4	5	6	7	8	9	10	11	12	Gesamt
3	1	0	0	0	0	0	0	0	0	0	1
4	7	0	0	0	0	0	0	0	0	0	7
5	12	4	0	0	0	0	0	0	0	0	16
6	23	19	1	0	0	0	0	0	0	0	43
7	47	55	3	0	0	0	0	0	0	0	105
8	84	144	27	0	0	0	0	0	0	0	255
9	172	314	146	14	0	0	0	0	0	0	646
10	335	619	492	99	2	0	0	0	0	0	1547
11	590	1179	1336	459	41	0	0	0	0	0	3605
12	1000	2102	3156	1714	262	7	0	0	0	0	8241
13	1858	3639	7082	5270	1340	89	1	0	0	0	19279
14	3284	6042	14938	14401	5359	655	27	0	0	0	44706
15	6083	9938	29282	36907	19210	3622	170	0	0	0	105212
16	10816	16202	55012	86696	60150	16348	1436	23	0	0	246683
17	19539	25758	100707	194306	172234	63635	8835	340	1	0	585355
18	35586	40685	178063	414660	460553	223997	44993	3058	49	0	1401644
19	65309	63343	306310	849564	1159167	720406	196391	20738	576	2	3381806
20	120625	98253	514381	1681744	2774702	2148017	762963	114232	5804	56	8220777
21	224763	151566	846627	3230120	6363475	6015901	2714473	547528	42764	983	20138200

C Verteilung von Lucas-Pseudoprimzahlen

Die Lucas-Pseudoprimzahlen wurden in Kapitel 2, Abschnitt X untersucht. Man erinnere sich daran, dass mit ganzen Zahlen P, Q ungleich Null und $D = P^2 - 4Q$ die Lucas-Folge definiert ist durch

$$U_0 = 0, \quad U_1 = 1, \quad U_n = PU_{n-1} - QU_{n-2} \quad (\text{für } n \geq 2),$$

und die zu D teilerfremde, zerlegbare Zahl n genau dann eine Lucas-Pseudoprimzahl (mit Parametern (P, Q)) ist, wenn gilt, dass $U_{n-(D|n)}$ von n geteilt wird.

Da der Begriff der Lucas-Pseudoprimzahl noch relativ neu ist, weiß man viel weniger über die Verteilung solcher Zahlen. Die hier verwendete Quelle ist der Artikel von Baillie & Wagstaff (1980), der schon in Kapitel 2 zitiert wurde. Hier die wesentlichen Resultate:

Die Anzahl $L\pi(x)$ von Lucas-Pseudoprimzahlen (mit Parametern (P, Q)) kleiner oder gleich x ist für genügend großes x beschränkt

durch

$$L\pi(x) < \frac{x}{e^{Cs(x)}},$$

wobei $C > 0$ eine Konstante ist und $s(x) = (\log x \log\log x)^{1/2}$.

Es folgt (wie in Szymiczeks Resultat für Pseudoprimzahlen) für beliebige Parameter (P, Q), dass $\sum(1/U_n)$ konvergent ist (Summation über alle Lucas-Pseudoprimzahlen mit diesen Parametern).

Andererseits zeigten Erdös, Kiss & Sárközy (1988), dass es eine Konstante $C > 0$ derart gibt, dass für jede nicht-entartete Lucas-Folge und genügend großes x gilt: $L\pi(x) > \exp\{(\log x)^C\}$.

Eine ähnliche untere Schranke existiert für die Anzahl $SL\pi(x)$ der starken Lucas-Pseudoprimzahlen (mit Parametern (P, Q)) kleiner oder gleich x (siehe die Definition in Kapitel 2, Abschnitt X): $SL\pi(x) > C' \log x$ (gültig für alle genügend großen x), wobei $C' > 0$ eine Konstante ist.