DIPLOMARBEIT

Anmerkungen zur Verteilung der Primzahlzwillinge

Autor: Andreas Piotrowski
Betreuer: Prof. Dr. Wolfgang Schwarz

Fachbereich Mathematik an der
Johann Wolfgang Goethe-Universität
Frankfurt am Main

Wintersemester 1999/2000

Zusammenfassung

Das Thema dieser Arbeit ist das Primzahlzwillingsproblem, d.h. das Problem der Bestimmung der Anzahl $\pi_d(N)$ von Primzahlen $p < N$, so daß auch die Zahl $p + d$ prim ist für eine fest gewählte gerade Zahl d. Im ersten Kapitel werden die wichtigsten historischen Ergebnisse vorgestellt, die zu oberen Abschätzungen von $\pi_d(N)$ geführt haben. Unter anderen wird ein für $d = 2$ existierendes Ergebnis von Brun auf alle geraden d verallgemeinert. Es ist bis heute unbekannt, ob eine wachsende untere Schranke existiert.

Im zweiten Kapitel wird ein kombinatorischer Ansatz des Autors vorgestellt, bei dem das Primzahlzwillingsproblem für $d = 2$ auf ein anderes Problem übertragen wird. Dabei wird nach einer Dualisierung des Primzahlzwillingsproblems die Anzahl von Paaren zusammengesetzter Zahlen kombinatorisch abgezählt und dann nach unten abgeschätzt. Daraus folgt anschließend eine untere Schranke für die Primzahlzwillinge ($d = 2$) mit einem kleinen Fehlerterm und einer unbekannten Funktion. Diese Funktion gibt dabei die Abweichung einer leicht berechenbaren mittleren Verteilung von Paaren aus zusammengesetzten Zahlen in einem großen Intervall von ihrer tatsächlichen Verteilung in einem kleineren Intervall an.

Im dritten und letzten Kapitel werden mit Hilfsmitteln der diskreten Fouriertransformation unter anderen die Formeln für die genaue Anzahl der Primzahlzwillinge ($d = 2$) zwischen einer festen Primzahl p und ihrem Quadrat p^2 sowie für eine charakteristische Funktion hergeleitet, die angibt, ob ein gegebenes Paar $(6n - 1, 6n + 1)$ nur Primzahlen enthält. Diese Formeln lassen sich anschließend auf eine Form bringen, die ohne Fourierkoeffizienten auskommt, die jedoch von den Teilern der Zahl $36n^2 - 1$ abhängt. Alle Formeln geben genaue Ergebnisse, erweisen sich aber gerade wegen ihrer Genauigkeit als (für den Autor) zu komplex für eine weitere Untersuchung beim Grenzübergang $n \to \infty$. Sie bringen jedoch neue Einsichten in die Gesetzmäßigkeiten der Bildung von Primzahlpaaren.

Erklärung zur Diplomarbeit

Hiermit erkläre ich, daß ich die vorliegende Arbeit selbständig abgefaßt und keine anderen Hilfsmittel als die angegebenen benutzt habe.

Ich erkläre ferner, daß diejenigen Stellen der Arbeit, die anderen Werken wörtlich oder dem Sinne nach entnommen sind, in jedem einzelnen Falle unter Angabe der Quellen kenntlich gemacht sind.

Frankfurt am Main
Dezember 1999

Andreas Piotrowski

Inhaltsverzeichnis

Kapitel 1

Siebtheoretische Ergebnisse und das Primzahlzwillingsproblem

1.1 Das Primzahlzwillingsproblem und verwandte Probleme

Obwohl es seit Euklid (3. Jahrh. v. Chr.) bekannt ist, daß es unendlich viele Primzahlen gibt, ist die sog. **Primzahlzwillingsvermutung** bis heute unbewiesen. Sie lautet folgendermaßen:

> "Es gibt unendlich viele Primzahlen p, so daß auch $p + 2$ eine Primzahl ist."

Obwohl der praktische Nutzen aus der Gewißheit, ob diese Vermutung auch richtig sei, nicht unbedingt auf der Hand liegt, hat sie wegen der Einfachheit ihrer Formulierung und der Schwierigkeit ihrer Bestätigung bzw. Widerlegung seit Jahrhunderten die Gemüter der Mathematiker fasziniert.

So weit die Berechnungen im Bereich der natürlichen Zahlen $\mathbb{N}$ reichen, tauchen immer wieder neue Primzahlzwillinge $(p, p + 2)$ auf. Die Suche nach immer größeren Primzahlzwillingen ist rechenaufwendig, und es bedarf eines gewissen Idealismus, um sich mit dieser profitlosen Kunst zu befassen. Die Ironie des Schicksals war es, daß gerade diese inprofitable Beschäftigung Milliardenverluste in der gesamten Computerbranche verursacht hat, als man bei der Berechnung der "Brunschen Konstante", die mit Primzahlzwillingen in

Zusammenhang steht, einen Hardwarefehler in der Recheneinheit der ersten Pentiumrechner entdeckte[1].

Die größten zur Zeit entdeckten Primzahlzwillinge (vgl. Caldwell [12]) sind die Zahlen

Zwillinge	Ziffern	Entdecker	Jahr
$361700055 \times 2^{39020} \pm 1$	11755	Lifchitz	1999
$835335 \times 2^{39014} \pm 1$	11751	Ballinger, Gallot	1998
$242206083 \times 2^{38880} \pm 1$	11713	Járai, Indlekofer	1995
$40883037 \times 2^{23456} \pm 1$	7069	Lifchitz, Gallot	1998
$843753 \times 2^{22222} \pm 1$	6696	Rivera, Gallot	1997

Die Primzahlzwillingsvermutung läßt sich für eine fest gewählte gerade Zahl d so verallgemeinern:

> "Es gibt unendlich viele Primzahlen p, so daß auch die Zahl p+d prim ist."

Im folgenden bezeichnen wir für jedes feste d das Problem, diese Vermutung zu beweisen oder zu widerlegen kurz als **PZd-Problem**, während wir Zahlenpaare $(p, p+d)$ mit der Eigenschaft, daß sowohl p als auch $p+d$ Primzahlen sind, **d-Zwillinge** nennen. Damit läßt sich die obere Vermutung auch so formulieren: Für eine (jede?) gerade Zahl $d \geq 2$ gibt es unendlich viele d-Zwillinge.

Hardy und Lord Cherwell vermuteten für die 2-Zwillinge die asymptotische Formel[2]

$$\pi_2(x) \sim \frac{2C_2 x}{\log^2 x} \text{ mit } C_2 = \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \approx 0.66016\ldots.$$

Daß diese Vermutung nicht unbegründet ist, zeigt die Tabelle 1.1. Dort wurde die Anzahl der Primzahlzwillinge $\pi_2(x)$ für $x \leq 10^9$ in Beziehung zum Verhältnis $x/\log^2 x$ gebracht. Berechnet wurde auch das Verhältnis

$$C(x) = \frac{\pi_2(x)\log^2(x)}{x},$$

von dem Hardy und Lord Cherwell vermuteten, daß es für $x \to \infty$ gegen die Konstante $2C_2$ konvergiert.

[1] vgl. Cipra [14].

[2] vgl. Hardy, Wright [22] S.467, teilweise ähnlich wie dort werden wir auch im Kapitel 2 und 3 argumentieren.

n	$\pi_2(10^n)$	$10^n/\log^2(10^n)$	$C(10^n)$
1	2	1.88611697	1.06037962
2	8	4.71529242	1.69660739
3	35	20.9568552	1.67009790
4	205	117.882310	1.73902257
5	1224	754.446788	1.62238082
6	8169	5239.21380	1.55920340
7	58980	38492.1830	1.53225915
8	440312	294705.776	1.49407318
9	3424506	2328539.46	1.47066693

Tabelle 1.1: Zur Hardy-Cherwellschen Vermutung. Rechenzeit auf einem Pentium 200MHz: ca 22,5 Stunden.

Der Satz 1.7.2, dessen Beweis in diesem Kapitel gebracht wird, liefert eine obere Schranke für die Anzahl solcher Zwillinge. Die dort vorkommende Konstante scheint nicht allzusehr von diesem asymtotischen Wert abzuweichen. Andererseits wurde wohl bemerkt bis heute weder eine untere Schranke der Form

$$C_1 \frac{x}{\log^2 x} \leq \pi_2(x)$$

bewiesen[3], noch hat man gezeigt, daß es überhaupt unendlich viele Primzahlzwillinge gibt. Solange es keinen Beweis gibt, nützt alle numerische Evidenz nichts.

Im Jahre 1923 stellten in [21] Hardy und Littlewood weitere Untersuchungen an, die den obigen Spezialfall $d = 2$ auf andere Werte für d-Zwillinge und selbst für Gruppen von 3 und mehr Primzahlen verallgemeinerten. Sie nannten dort 15 Vermutungen. Die Vermutung B ihrer Arbeit betrifft die d-Zwillinge und sagt aus, daß für ihre Anzahl

$$\pi_d(x) := \#\{p + d \leq x : \; p, p + d \; prim\}$$

die folgende asymptotische Formel gilt

$$\pi_d(x) \sim 2C_2 \frac{x}{\log^2 x} \prod_{p|d, p>2} \frac{p-1}{p-2} \tag{1.1}$$

[3]also mit $0 < C_1 < C$, falls Hardy und Lord Cherwell Recht hatten.

gilt. Diese sogenannte **Hardy-Littlewoodsche Vermutung Nr. B** widerstrebt bis heute allen Beweisversuchen, sie läßt sich jedoch numerisch ziemlich genau untermauern[4]. Einige numerische Analysen werden auch im 2. Kapitel vorgestellt.

Da für Teilbarkeitsuntersuchungen die Vorzeichen offenbar keine Rolle spielen, kann man den Primzahlbegriff auf alle ganzen Zahlen $\mathbb{Z}$ ausdehnen. So sind dann auch $-2, -3, -5, \ldots$ Primzahlen. Mit dieser Verallgemeinerung wird die Verwandtschaft des PZd-Problems mit der genauso berühmten **Goldbachschen Vermutung** deutlich:

> "Jede genügend große gerade natürliche Zahl läßt sich als Summe zweier Primzahlen darstellen."

Sind nämlich p und $p+d$ Primzahlen, so ist ihre Summe $N = 2p+d$ eine gerade Zahl. Aus der Richtigkeit der Primzahlzwillingsvermutung für mindestens ein $d \geq 2$ würde also folgen, daß für unendlich viele geraden Zahlen eine Summe der Form $N = p+p'$ gefunden werden kann. Daraus würde aber nicht einmal folgen, daß dies für fast alle geraden Zahlen der Fall sein müßte. Tatsächlich gelang es Karl Prachar 1954 zu zeigen, daß es unendlich viele gerade N gibt, für die die Anzahl der Darstellungen als Summe zweier Primzahlen $N = p+p'$ durch

$$c\frac{N}{\log^2 N} \log\log N$$

nach unten abgeschätzt werden kann[5]. Er konnte es jedoch nicht für fast alle N (also alle bis auf endlich viele Ausnahmen) zeigen.

Wäre umgekehrt jede genügend große gerade Zahl $N = p + p'$ Summe von zwei Primzahlen, so folgt daraus für zwei Primzahlen $-p' = p - N$. Ist o.B.d.A. $p' < p$, so kann dann mit $d := N - 2p'$ der Zwilling $p', p' + d = p$ gefunden werden.

Obwohl das ursprüngliche Goldbachsche Problem noch auf seine Lösung wartet, konnte Vinogradoff 1937 zeigen, daß jede genügend große ungerade Zahl sich als Summe von 3 Primzahlen darstellen läßt, in dem er zuerst dieses an sich diophantische Problem als Integral über ein trigonometrisches Polynom modellierte und dieses Integral dann asymtotisch lösen konnte (vgl. Brüdern [5] Kap 6.4 oder Originalarbeit Vinogradoff [40]).

[4] vgl. z.B. Nycely [29] oder Wolf [41]

[5] vgl. Prachar [32], S. 152.

Nach dem Fundamentalsatz der Zahlentheorie läßt sich bekanntlich jede natürliche Zahl als Produkt von Primzahlen darstellen. Eine ganze Zahl P_m nennt man **Fastprimzahl**, falls sie höchstens m nicht unbedingt verschiedene Primfaktoren besitzt.

Lange Zeit dachte man, die gegenwärtige Mathematik verfüge über zu schwache Hilfsmittel, um das PZd-Problem anzugreifen. 1919 gelang jedoch Viggo Brun ein bemerkenswerter neuartiger Zugang zu diesem Problem: Er zeigte, daß es unendlich viele Fastprimzahlen $n, n+2$ gibt, von denen jede höchstens 9 Primfaktoren hat, also ein P_9 ist. Entsprechend konnte er zeigen, daß für alle genügend großen geraden Zahlen N es stets eine Summenzerlegung $N = P_9 + P_9$ gibt[6]. Brun gelang es auch als erstem, eine obere Schranke für die Anzahl der 2-Zwillinge zu finden (Brun [6]) und hat sie anschließend noch verbessert. Dieselbe Verbesserung gelang 1947 A. Selberg mit einer anderen, von ihm entwickelten Siebmethode für obere Schranken, die wegen ihrer Einfachheit berühmt geworden ist.

Im Jahre 1950 zeigte Selberg mit einer speziell für untere Schranken entwickelten Methode, daß für unendlich viele n der Polynomwert $n(n+2)$ höchstens ein P_5 ist, daß es also unendlich viele Zwillinge der Form (p, P_4), $(P_2, P_3), \dots, (P_4, p)$ gibt, doch schon 1947 gelang es Rényi [33] mit tiefer liegenden Methoden für das Goldbachsche Problem zu zeigen, daß man eine der Zahlen als wirklich prim voraussetzen kann. Er zeigte, daß eine Konstante $c \in \mathbb{N}$ existiert, so daß für genügend große geraden N stets eine Gleichung $N = p + P_c$ gefunden werden kann.

Das Goldbasche und das PZd-Problem sind Spezialfälle einer noch allgemeineren Vermutung: Angenommen, das Polynom $h(n)$ sei ein Produkt von paarweise verschiedenen irreduziblen Polynomen $h_1(n), \dots, h_j(n) \in \mathbb{Z}[X]$, und es gebe keine feste Primzahl p, die alle Polynomwerte von $h(n)$ teilt. Das PZd-Problem läßt sich nun verallgemeinern, indem man die folgende Behauptung aufstellt:

> "Es gibt unendlich viele n, so daß alle Werte $h_i(n)$ für $i = 1, \dots, j$ gleichzeitig prim werden."

Sei $g(n)$ ein anderes ganzzahliges Polynom, so daß $N - g(n)$ irreduzibel ist und $h(N - g(n))$ keinen festen Primteiler hat. Dann läßt sich die Goldbachsche Vermutung folgendermaßen generalisieren:

---

[6] Ein verbessertes Ergebnis $N = P_7 + P_7$, das ebenfalls mit der Brunschen Siebmethode erzielt werden kann, findet man in Halberstam, Richert [19], Kap. 2.

> "Für genügend große N findet man stets Argumente n, so daß sowohl $h_i(n)$ für $i = 1, \dots, j$ als auch $N - g(n)$ gleichzeitig prim werden[7]."

Eine relativ gute obere Schranke für die Anzahl der n, für die beide Vermutungen richtig sind, folgt schon aus der Selbergschen Siebmethode für obere Schranken. Doch mit Hilfe des gewichteten Siebes, einer Weiterentwicklung der Selbergschen Methode für untere Schranken, die Halberstam und Richert[8] 1974 und vielen anderen zuvor (vgl. z.B. Buchstab [9], Ankeny und Onishi [2]) gelungen ist, kann man viel schwieriger nachzuweisende untere Schranken für beide Vermutungen in einer abgeschwächten Form finden, wobei in beiden das Wort "prim" durch "eine Fastprimzahl P_r" zu ersetzen ist. Mit ihren rechenintensiven Methoden folgt zum Beispiel, daß $n(n+d) = P_3$ für unendlich viele n gilt und daß für alle genügend großen geraden N stets eine Summe $N = p + P_3$ gefunden werden kann.

Unabhängig von Halberstam und Richert konnte 1973 Jing-run Chen nach ähnlich aufwendigen Berechnungen diese Ergebnisse auf einen P_2 verbessern[9]. Dies ist bis heute das beste Ergebnis und die beste bekannte Näherungslösung des PZd- und des Goldbachschen Problems.

In diesem Kapitel werden zuerst die kombinatorischen Einzelheiten des Siebprozesses erläutert, und es wird erklärt, warum diese Methode für Primzahlzwillinge nicht funktioniert. Anschließend wird der erste von Brun erzielte Fortschritt für das Finden oberer Schranken für den Fall $d = 2$ auf beliebige d-Zwillinge verallgemeinert. Danach wird die Siebmethode von Selberg für obere Schranken vorgestellt, mit der sich ein besseres Ergebnis erzielen läßt. Schließlich folgt ein kurzer Bericht über die Methoden, die erst in neuerer Zeit für untere Schranken entwickelt worden sind und die relativ viele komplizierte Berechnungen erfordern, auf die hier aus Platzgründen verzichtet wird.

1.2 Notation

Im folgenden Text werden viele gängige Bezeichnungen und Symbole benutzt, ohne daß für sie explizit eine Definition im Text angegeben wird. Eigenständi-

[7] Man erkennt für $j = 1$, $h_1(n) = g(n) = n$ die Goldbachsche Vermutung wieder. Diese Verallgemeinerungen findet man in Halberstam, Richert[19], Introduction.

[8] vgl. [19]

[9] vgl. Chen [13]

ge Definitionen werden nur für spezielle Größen angegeben, die im folgenden Text neu eingeführt werden. Die folgende Auflistung enthält beide Symbolarten und soll als Referenz für alle häufig benutzten Größen verstanden werden.

Innerhalb eines Kapitels sind die Nummern von Abschnitten, Tabellen, Abbildungen und einzelnen Zeilengleichungen zweistellig, die Nummern von Sätzen, Definitionen und Lemmata dreistellig. Wird im Text in einem Kapitel auf Abschnitte oder Sätze eines anderen Kapitels verwiesen, wird diesem Verweis die Nummer des Kapitels vorangestellt.

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ Mengen der natürlichen, ganzen, rationalen, reellen und komplexen Zahlen respektive.

$\Re(z)$, $\Im(z)$ Real- und Imaginäranteil der komplexen Zahl z.

$\mathrm{ggT}(n,m)$ größter gemeinsamer Teiler der ganzen Zahlen n, m mit positiven Vorzeichen.

$\mathrm{kgV}(n,m)$ kleinstes gemeinsames Vielfaches der ganzen Zahlen n, m mit positiven Vorzeichen.

$\mathrm{gPf}(n)$ größter positiver Primfaktor von n.

$\mathrm{kPf}(n)$ kleinster positiver Primfaktor von n.

$\Omega(n)$ Anzahl der Primteiler von $n \in \mathbb{N}$.

$\omega(n)$ Anzahl der verschiedenen Primteiler von $n \in \mathbb{N}$.

$\mu(n)$ Möbiussche μ-Funktion. Es gilt:

$$\mu(n) := \begin{cases} 1, & \text{falls } n \text{ quadratfrei und } \omega(n) \text{ gerade ist,} \\ -1, & \text{falls } n \text{ quadratfrei und } \omega(n) \text{ ungerade ist,} \\ 0 & \text{sonst, also falls } n \text{ nicht quadratfrei ist.} \end{cases}$$

$\phi(n)$ Eulersche ϕ-Funktion; gibt die Anzahl der natürlichen Zahlen $a \leq n$ an mit $\mathrm{ggT}(a,n) = 1$.

h Dieser Buchstabe bezeichnet ausschließlich Polynome $h = h(m) \equiv \prod_{i=1}^{j} h_i(m)$ mit ganzzahligen Koeffizienten. Dabei wird verlangt, daß alle h_i irreduzibel im Polynomenring $\mathbb{Z}[X]$ sind und daß h streng monoton wachsend auf $\mathbb{N}$ ist.

$\phi_h(n)$ Bezeichnet die Anzahl der $m = 1, \ldots, n$ mit $\mathrm{ggT}(n, h(m)) = 1$. (Insofern eine Verallgemeinerung der Eulerschen ϕ-Funktion, wenn man $\phi(n) = \phi_m(n)$ setzt).

$\Phi_h(n)$ Zählt die Anzahl der i-Tupel $(h_1(m), \ldots, h_i(m))$ für $m = 1, \ldots, n$, für die gleichzeitig $\mathrm{ggT}(h_1(m), n) > 1, \ldots, \mathrm{ggT}(h_i(m), n) > 1$ gilt.

P_d eine beliebige ganze Zahl mit maximal $d \geq 1$ (nicht unbedingt verschiedenen) Primteilern. Insofern ist jedes P_1 entweder 1 oder eine Primzahl, ein P_2 entweder 1 oder Primzahl oder Produkt zweier Primzahlen, usw.

$\mathbb{P}_d$ bezeichnet die Menge aller Primzahlen p, die $d \in \mathbb{N}$ nicht teilen, also $p \in \mathbb{P}_d \implies p \nmid d$.

$\mathbb{N}_d$ steht für alle natürlichen Zahlen, die zu $d \in \mathbb{N}$ teilerfremd sind, also aus $n \in \mathbb{N}_d$ folgt $\mathrm{ggT}(n, d) = 1$. Insofern ist $\mathbb{P}_d \subset \mathbb{N}_d$. Man überlegt sich weiter leicht, daß $\mathbb{N}_d \cup \{1\}$ eine teilegeschlossene Menge bildet, die genau von den Primzahlen aus $\mathbb{P}_d$ erzeugt wird. Insbesondere gilt $\mathbb{N} = \mathbb{N}_1$.

$\mathbb{P}$ bezeichnet die Menge aller Primzahlen (insbesondere gilt also $\mathbb{P} = \mathbb{P}_1$).

$\pi_d(n)$ steht für die Anzahl der Primzahlpaare $(p, p + d)$ mit $p + d \leq n$.

$\pi(n)$ steht für die Anzahl der Primzahlen $\leq n$.

$[a, b]$ steht für das Intervall $\{x \in \mathbb{R},\ a \leq x \leq b\}$.

$]a, b[$ steht für das Intervall $\{x \in \mathbb{R},\ a < x < b\}$.

$\lfloor a \rfloor$ bezeichnet die größte ganze Zahl $\leq a \in \mathbb{R}$.

$f(n) = \mathcal{O}(g(n))$ (manchmal schreiben wir hier auch $f(n) \ll g(n)$ oder $g(n) \gg f(n)$); bedeutet, daß für $n \to \infty$ eine positive Konstante K existiert mit $|f(n)| \leq K \cdot |g(n)|$. Salopp ausgedrückt: $|f(n)|$ wächst bis auf einen konstanten von n unabhängigen Faktor langsamer (fällt bis auf einen konstanten Faktor schneller) als die wachsende (fallende) Funktion $|g(n)|$. So bedeutet etwa $f(n) \ll 1$, daß $f(n)$ beschränkt ist.

$f(n) = o(g(n))$ bedeutet, daß für $n \to \infty$ das Verhältnis $f(n)/g(n)$ gegen Null geht. Salopp ausgedrückt: $|f(n)|$ wächst viel langsamer (oder wird viel schneller kleiner) als $|g(n)|$. Zum Beispiel bedeutet $f(n) = o(1)$, daß $f(n)$ eine Nullfolge ist. $f(n) \ll g(n)$ ist notwendig aber nicht hinreichend für $f(n) = o(g(n))$.

1.3 Formulierung des allgemeinen Siebproblems

In dieser Arbeit spielt der Siebbegriff eine zentrale Rolle. In der Literatur findet man verschiedene Siebdefinitionen, die mehr oder weniger allgemein gefaßt sind. Die wohl allgemeinste findet man etwa in Schwarz [35] S. 163ff oder Halberstam/Roth [20] S. 204ff, die hier in einer etwas abgewandelten Form zur Einführung gegeben werden soll. Gegeben sei eine endliche Folge

$$\mathcal{A} =: \{a_1 < a_2 < \cdots < a_N\}$$

natürlicher Zahlen und eine geordnete endliche Primzahlmenge

$$\mathcal{P} := \{p_1 < p_2 < \cdots < p_\rho\}.$$

Jeder Primzahl $p_r \in \mathcal{P}$ seien k_r inkongruente Restklassen modulo p_r zugeordnet, die hier mit $R_r^{(1)}, \ldots, R_r^{(k_r)}$ bezeichnet werden mögen. Ferner sei

$$\mathcal{R} := \bigcup_{r=1}^{\rho} \bigcup_{j=1}^{k_r} R_r^{(j)}$$

die Vereinigung aller dieser Restklassen.

Definition 1.3.1 *Das Tripel* $(\mathcal{A}, \mathcal{P}, \mathcal{R})$ *nennen wir das zugehörige* ***Sieb****, und unter* $S(N)$ *verstehen wir die Anzahl der Zahlen in* $\mathcal{A}$*, die in keine der Restklassen in* $\mathcal{R}$ *fallen, in anderen Worten setzen wir*

$$S(N) := \#\{n \leq N : a_n \notin \mathcal{R}\}. \tag{1.2}$$

Das zugehörige ***Siebproblem*** *ist das Problem,* $S(N)$ *möglichst genau nach oben und unten abzuschätzen.*

Der Siebprozeß selbst hat eine kombinatorische Natur. Man stelle sich endliche Zahlenmengen $\mathcal{B}_1, \ldots, \mathcal{B}_\rho$ vor mit den Kardinalitäten $\#\mathcal{B}_1, \ldots, \#\mathcal{B}_\rho$. Alles reduziert sich auf die Beantwortung der folgenden Frage: Wie groß ist die Anzahl der Zahlen in der Vereinigung

$$\mathbf{B} := \bigcup_{r=1}^{\rho} \mathcal{B}_r \text{ ?}$$

wobei natürlich alle B_r nichtdisjunkte Mengen sind, denn sonst wäre das Problem trivial.

Bei unserem Sieb sind die Mengen B_r diejenigen Zahlen $a_1, \ldots, a_N$, die in *eine bestimmte* Restklasse aus den k_r zur Verfügung stehenden Restklassen $R_r^{(1)}, \ldots, R_r^{(k_r)}$ modulo der Primzahl p_r fallen, $r = 1, \ldots, \rho$. Die Vereinigung dieser Mengen entspricht dann allen $a \in \mathcal{A}$, die in mindestens eine der Restklassen aus $\mathcal{R}$ fallen, und deshalb gilt für unser Sieb

$$S(N) = N - \#\mathbf{B}. \tag{1.3}$$

Obwohl man so die Natur des Problems besser versteht und sogar eine "Formel" für $\#\mathbf{B}$ kennt, die sich kombinatorisch aus dem Einschluß-Ausschluß-Prinzip ergibt[10]:

$$\begin{aligned} \#\mathbf{B} &= \sum_{r=1}^{\rho} \#\mathcal{B}_r \\ &- \sum_{1 \leq r < s \leq \rho} \#(\mathcal{B}_r \cap \mathcal{B}_s) \\ &+ \sum_{1 \leq r < s < t \leq \rho} \#(\mathcal{B}_r \cap \mathcal{B}_s \cap \mathcal{B}_t) \\ &\vdots \\ &+ (-1)^{\rho-1} \#(\mathcal{B}_1 \cap \ldots \cap \mathcal{B}_\rho), \end{aligned}$$

führt diese Formel nicht zum Erfolg, da man nur schwer, wenn überhaupt, die Kardinalitäten der auftauchenden Durchschnitte bestimmen kann, und wenn es doch möglich ist, scheitert das Verfahren an der ungeheuer großen Anzahl der Summanden in dieser Formel[11].

Mit der Möbiusschen μ-Funktion

$$\mu(n) := \begin{cases} 1, & \text{falls } n \text{ quadratfrei und } \omega(n) \text{ gerade ist,} \\ -1, & \text{falls } n \text{ quadratfrei und } \omega(n) \text{ ungerade ist,} \\ 0 & \text{sonst, also falls } n \text{ nicht quadratfrei ist,} \end{cases}$$

kann man die Sylvester-Formel auf die Bedürfnisse der Siebtheorie zuschneiden, was im folgenden Lemma (vgl. Prachar [31] S. 32ff) geschehen soll. Quadratfrei bedeutet, daß jeder Primteiler $p|n$ nur in der ersten Potenz in

[10] sog. Formel von Sylvester

[11] Bei ρ Primzahlen gibt es $2^\rho - 1$ Summanden.

der Primzerlegung von n vorkommt, daß also zwar $p|n$ aber schon $p^2 \nmid n$ gilt. Ferner bezeichnet $\omega(n)$ die Anzahl der verschiedenen Primteiler von $n \in \mathbb{N}$. Doch nun zum angekündigten

Lemma 1.3.1 *Sei $\mathcal{K} := \{k_1, \ldots, k_N\}$ eine Menge nicht unbedingt verschiedener natürlicher Zahlen und $f(k)$ eine beliebige arithmetische Funktion*[12]*. Sei T das Produkt aller Primzahlen, die mindestens ein $k \in \mathcal{K}$ teilen. Ferner seien $\mathcal{K}_t$ diejenigen Teilmengen von $\mathcal{K}$, deren Zahlen durch $t \in \mathbb{N}$ teilbar sind. Sei für jedes solche $t \geq 1$*

$$S_t := \sum_{k \in \mathcal{K}_t} f(k)$$

und sei

$$S := \sum_{\substack{k \in \mathcal{K} \\ k=1}} f(k).$$

Dann gilt

$$S = \sum_{t|T} \mu(t) S_t. \tag{1.4}$$

Beweis: Die Definition von S besagt also, daß über alle $k \in \mathcal{K}$ summiert wird, die gleich 1 sind. Wir bemerken ferner, daß $\mathcal{K}_1 = \mathcal{K}$ ist. Die Behauptung ergibt sich dann sofort durch Vertauschung der Summationsreihenfolge in

$$\begin{aligned} S &= \sum_{\substack{k \in \mathcal{K}_1 \\ k=1}} f(k) = \sum_{k \in \mathcal{K}_1} f(k) \sum_{t|k} \mu(t) \\ &= \sum_{t|T} \mu(t) \sum_{k \in \mathcal{K}_t} f(k) = \sum_{t|T} \mu(t) S_t \end{aligned}$$

□

Im Beweis wurde eine sehr wichtige Eigenschaft der μ-Funktion benutzt, die man folgendermaßen ausdrücken kann:

$$\sum_{t|k} \mu(t) = \begin{cases} 1, & \text{falls } k = 1 \\ 0, & \text{falls } k > 1. \end{cases} \tag{1.5}$$

[12] Unter arithmetischen Funktionen versteht der Verfasser alle Abbildungen, die jeder natürlichen Zahl eine beliebige komplexe Zahl zuordnen.

Dieses Ergebnis hat ebenfalls einen kombinatorischen Charakter[13]. Aufgrund der Definition von μ reicht es, in der Summe nur quadratfreie Teiler $t|k$ zu betrachten. Ist $\omega(k)$ die Anzahl der verschiedenen Primteiler von k, dann kann man alle Teiler $t|k$ so gruppieren, daß sie selbst jeweils $0, 1, \ldots, \omega(k)$ Primteiler haben. Nun ist $\mu(t) = -1$, falls diese Anzahl ungerade, und $\mu(t) = 1$, falls sie gerade ist. Da es jeweils $\binom{\omega(k)}{j}$ Teiler t mit genau j verschiedenen Primteilern gibt, erhalten wir

$$\sum_{t|k} \mu(t) = \sum_{j=0}^{\omega(k)} \binom{\omega(k)}{j} (-1)^j = (1-1)^{\omega(k)}$$

und daraus die Behauptung. Um den Kreis zu schließen, weisen wir auf den Zusammenhang zwischen dem Lemma 1.3.1 und der Sylvester-Formel hin. Dazu setzen wir in diesem Lemma

$$k_i = \begin{cases} 1, & \text{falls } a_i \notin \mathcal{R} \\ p_{r_1} \cdots p_{r_j}, & \text{falls } a_i \text{ modulo jeder der } j \text{ Primzahlen} \\ & p_{r_1}, \ldots, p_{r_j} \text{ in eine Restklasse fällt und es keine} \\ & \text{anderen Primzahlen dieser Art gibt,} \end{cases}$$

und $f(k_i) = 1$ für alle $i = 1, \ldots, N$. Betrachten wir nun zum besseren Verständnis die verschiedenen Fälle: S_t stellt die Anzahl derjenigen Zahlen in $\mathcal{K}$ dar, die durch t teilbar sind, also auch die Anzahl derjenigen Zahlen in $\mathcal{A}$, die in eine der Resklassen modulo jeder Primzahl p fallen, die t teilen. Ist $t = 1$, so stellt S_1 die Anzahl derjenigen Zahlen in $\mathcal{K}$ dar, die durch 1 teilbar sind, also N, was auch gleich der Anzahl aller $a \in \mathcal{A}$ ist. Nun zählt die Größe S aus Lemma 1.3.1 nur die k_i, die gleich 1 sind, was wiederum der Anzahl derjenigen $a \in \mathcal{A}$ entspricht, die in keine der Restklassen aus $\mathcal{R}$ fallen, also unsere Siebgröße $S(N)$. Alles in allem entspricht die Formel (1.4) genau der Formel (1.3)[14].

Obwohl wir bisher versucht haben, das Siebproblem so allgemein wie möglich darzustellen, ist es angebracht, jetzt schon die anstehenden Vereinfachungen vorwegzunehmen: In den Abschnitten 1.4 und 2.2.1 wird sich herausstellen, daß es für das PZd-Problem ausreicht, die Folge $\mathcal{A}$ als Werte

[13] Die Formel (1.5) könnte tatsächlich auch als rekursive Definition der μ-Funktion benutzt werden: Man berechne $\mu(k)$, indem man zuerst $\mu(t)$ für alle Teiler $t \neq k$ nach der Formel berechnet mit dem induktiven Anfang $\mu(1) = 1$. Vgl. auch [18] S.136 ff

[14] Man könnte sogar so weit gehen, daß man in den beiden Formeln Summanden zueinander eindeutig zuordnet.

eines ganzzahligen Polynoms $h(\nu)$ aufzufassen. Dann reicht es auch, für jede Primzahl $p_r|T$ nur eine einzige Restklasse - die Restklasse $0 \mod p_r$ - in Betracht zu ziehen.

Wir greifen deshalb auf die Siebdefinition in Halberstam, Roth [20] zurück[15], die für die folgenden Ausführungen vollkommen ausreichen wird.

Definition 1.3.2 *Seien $\mathcal{A} := \{a_1, \ldots, a_N\}$ eine Folge diskreter ganzer (nicht unbedingt positiver) Zahlen*[16] *und $z \geq 2$ eine reelle, $d \geq 1$ eine natürliche Zahl. Ferner sei $\mathbb{P}$ die Menge aller Primzahlen und $\mathbb{P}_d$ die Menge aller Primzahlen, die d nicht teilen. Schließlich setzen wir*

$$P(z) := \prod_{\substack{p \in \mathbb{P}_d, \\ p \leq z}} p.$$

*Dann nennen wir das Tripel $(\mathcal{A}, \mathbb{P}_d, z)$ ein **Sieb** und bezeichnen mit*

$$S(\mathcal{A}, \mathbb{P}_d, z) := \#\{a \in \mathcal{A},\ \mathrm{ggT}(a, P(z)) = 1\} \tag{1.6}$$

*die Anzahl derjenigen $a \in \mathcal{A}$, die zu $P(z)$ teilerfremd sind. Das zugehörige **Siebproblem** ist das Problem, $S(\mathcal{A}, \mathbb{P}_d, z)$ möglichst genau nach oben und unten abzuschätzen.*

Die Siebtheorie hat in der zweiten Hälfte des 20. Jahrhunderts viele Fortschritte gemacht. Eine gute Übersicht über die Methoden zur Lösung des Siebproblems und der Anwendung der Siebtheorie auf viele zahlentheoretische Probleme (das PZd-Problem eingeschlossen) findet man z.B. im Buch von Halberstam und Richert [19]. Einen Überblick über einige Siebmethoden kann sich der Leser auch im Buch von Schwarz [35] verschaffen.

Der Rest des Kapitels ist einigen Methoden gewidmet, die im Laufe der Zeit entwickelt wurden und die auf das PZd-Problem anwendbar sind.

1.4 Naive Anwendung der Siebmethode

In diesem Abschnitt wollen wir das Lemma 1.3.1 auf das PZd-Problem übertragen. Obwohl das Lemma allgemein auf Siebprobleme anwendbar ist, werden wir hier feststellen, daß diese zunächst auf der Hand liegende Vorgehensweise schnell auf ihre Grenzen stößt.

[15] Dort findet man eine etwas abweichende Definition von $P(z)$, wo z als Oberschranke nicht zugelassen wird.

[16] Meist werden es die Werte eines entsprechenden ganzzahligen Polynoms $h(\nu)$ sein.

Sei im folgenden $d \geq 2$ gerade. Wir betrachten das Polynom $h(\nu) = \nu(\nu+d)$ und setzen

$$\mathcal{A} := \{a_\nu = h(\nu), \nu = 1, \ldots, N\}.$$

Wir bemerken, daß der Wert von $h(\nu)$ das Produkt zweier d-Zwillinge sein muß, falls es keinen Teiler hat, der $\leq \sqrt{N+d}$ ist[17]. Um das Lemma 1.3.1 anwenden zu können, setzen wir

$$\mathcal{K} := \{\mathrm{ggT}(a_\nu, P(z)), \nu = 1, \ldots, N\},$$

wobei wir für $P(z)$ alle Primzahlen aus $\mathbb{P}_1 = \mathbb{P}$ zulassen und den Parameter $z \geq 2$ erst später festlegen werden[18]. Wie schon früher, führen wir für alle Teiler $t|P(z)$ die Mengen $\mathcal{A}_t \subseteq \mathcal{A}$ und $\mathcal{K}_t \subseteq \mathcal{K}$ ein mit Gleichheit im Falle $t = 1$. Dabei bezeichnen $\mathcal{A}_t$ diejenigen $a \in \mathcal{A}$, die durch t teilbar sind. Die $\mathcal{K}_t$ stimmen mit den $\mathcal{A}_t$ für alle $t \geq 1$ nicht nur in den Kardinalitäten überein. Es gilt überdies $k_\nu = 1 = a_\nu$ im Falle $\mathrm{ggT}(a_\nu, P(z)) = 1$ und falls $\mathrm{ggT}(a_\nu, P(z) > 1$ ist, dann ist k_ν der größte quadratfreie Teiler von a_ν[19]. Insofern haben wir die $\mathcal{A}_t$ sozusagen in den $\mathcal{K}_t$ von quadratvollen Zahlen bereinigt.

Ferner setzen wir $f(k) = 1$ für alle $k \in \mathcal{K}$. Nach dem Lemma 1.3.1 gilt dann

$$S = S(N) = \sum_{t|P(z)} \mu(t) \sum_{k \in \mathcal{K}_t} 1. \tag{1.7}$$

Wir brauchen zunächst also eine gute Abschätzung für die Zahlen $S_t = \sum_{k \in \mathcal{K}_t} 1$. Wie man sehen kann, zählen sie, wie oft die Kongruenz

$$\nu(\nu+d) \equiv 0 \bmod t, \qquad \nu = 1, \ldots, N$$

erfüllt ist für die (quadratfreien) Teiler $t|P(z)$.

Relativ trivial ist die folgende Aussage, die hier ohne Beweis angeführt wird[20].

[17] Denn sonst wäre eine der Zahlen ν oder $\nu + d$ zusammengesetzt.

[18] Es liegt auf der Hand, daß man hier zuerst $z = \sqrt{N+d}$ versuchen kann.

[19] Das folgt daraus, daß alle Teiler von $P(z)$ quadratfrei sind und deshalb auch alle $\mathrm{ggT}(a_\nu, P(z))$.

[20] vgl. Schwarz [35], S. 41

Lemma 1.4.1 *Ist h ein ganzzahliges Polynom, ist t quadratfrei, und bezeichnet $\beta(t)$ die Anzahl aller inkongruenter Lösungen ν der Kongruenz $h(\nu) \equiv 0(t)$, $\nu = 1, \ldots, t$, so gilt*

$$R_t := \left| \#\{\nu \leq N,\ h(\nu) \equiv 0 \bmod t\} - N\frac{\beta(t)}{t} \right| \leq \beta(t).$$

□

Damit läßt sich die ad-hoc Abschätzung

$$\begin{aligned} S = S(N) &= N \sum_{t|P(z)} \mu(t)\frac{\beta(t)}{t} + \mathcal{O}\left(\left| \sum_{t|P(z)} \mu(t) R_t \right| \right) \\ &= N \sum_{t|P(z)} \mu(t)\frac{\beta(t)}{t} + \mathcal{O}\left(\sum_{t|P(z)} R_t \right) \end{aligned} \tag{1.8}$$

gewinnen. Dabei gilt $0 \leq R_t \leq \beta(t)$.

Man kann sich nun leicht überlegen, daß für Primzahlen p gelten muß

$$\beta(p) = \begin{cases} 1, & \text{falls } p|d \\ 2 & \text{sonst, also falls } p \in \mathbb{P}_d. \end{cases} \tag{1.9}$$

Elementar ist nun das folgende

Lemma 1.4.2 *Seien $t = t_1 \cdots t_k$ und die ganzen Zahlen $t_1, \ldots, t_k$ paarweise relativ prim, und sei $h(\nu)$ ein Polynom mit ganzzahligen Koeffizienten. Gibt es für $i = 1, \ldots, k$ jeweils $\beta(t_i)$ verschiedene Kongruenzklassen $\nu \in \mathbb{Z}_{t_i}$, die die Kongruenzen $h(\nu) \equiv 0 \bmod t_i$ lösen, dann gibt es genau $\beta(t) = \beta(t_1) \cdots \beta(t_k)$ inkongruente Restklassen $\nu \in \mathbb{Z}_t$, die die Kongruenz $h(\nu) \equiv 0 \bmod t$ lösen.*

Beweis: Vgl. beispielsweise Jones & Jones [25], S.58.

□

Bemerkung: In anderen Worten bedeutet es, daß β eine sog. multiplikative Funktion ist. Eine arithmetische Funktion $f : \mathbb{N} \to \mathbb{C}$ heißt **multiplikativ** wenn für ggT(m, n) stets $f(mn) = f(m)f(n)$ gilt. Sie heißt **total multiplikativ**, falls die Gleichung $f(mn) = f(m)f(n)$ ohne jede Einschränkung

erfüllt ist[21].
Nach dem Lemma 1.4.2 gilt für quadratfreie t

$$\beta(t) = \prod_{p|t} \beta(p) \tag{1.10}$$

und deshalb ist

$$\sum_{t|P(z)} \mu(t)\frac{\beta(t)}{t} = \prod_{p|P(z)} \left(1 - \frac{\beta(p)}{p}\right) = C_d \cdot \prod_{\substack{2\le p\le z\\ p\in\mathbb{P}_d}} \left(1 - \frac{2}{p}\right) \tag{1.11}$$

mit der von d abhängigen Konstanten[22]

$$C_d := \prod_{\substack{2\le p\le z\\ p\notin\mathbb{P}_d}} \left(1 - \frac{1}{p}\right).$$

Aus (1.8) und (1.11) ergibt sich dann

$$S = S(N) = C_d N \prod_{\substack{2\le p\le z\\ p\in\mathbb{P}_d}} \left(1 - \frac{2}{p}\right) + \mathcal{O}\left(\sum_{t|P(z)} \beta(t)\right). \tag{1.12}$$

Schließlich erhalten wir mit Lemma 1.4.3 für $z = \sqrt{N+d}$ und $b = 2$ den folgenden Ausdruck für $\pi_d(x)$:

$$\pi_d(N+d) = C_d' \frac{N}{\log^2 N} + \mathcal{O}\left(\sum_{t|P(\sqrt{N+d})} \beta(t)\right) + \mathcal{O}\left(\sqrt{N}\right) \tag{1.13}$$

mit einer weiteren nur von d abhängigen Konstanten C_d'. Der Restterm $\mathcal{O}\left(\sqrt{N}\right)$ steht für die Anzahl der d-Zwillinge, die $\le \sqrt{N+d}$ sind und nicht von $S(N)$ gezählt werden. Dieser Restterm ist jedoch vernachlässigbar gegenüber der Summe

$$\sum_{t|P(z)} \beta(t) > \sum_{t|P(z)} 1 = 2^{\pi(z)},$$

[21] In der Sprache der Algebra ist dann also f ein **Homomorphismus** von $\mathbb{N}$ nach $\mathbb{C}$

[22] O.b.d.A. seien z und N so groß gewählt, daß alle Primteiler von d kleiner oder gleich z sind - ansonsten können wir nicht alle d-Zwillinge bis $N+d$ erfassen.

wobei $\pi(z)$ die Anzahl der Primzahlen $\leq z$ bezeichnet. Nach bekannten Abschätzungen für $\pi(z)$ erreicht der Fehlerterm[23] für die Wahl $z = \sqrt{N+d}$ die Größenordnung $2^{c\sqrt{N}/\log N}$, welche die des Hauptglieds $C_d'' \frac{N}{\log^2 N}$ bei weitem übertrifft, so daß die ganze Rechnung vorerst in einer Sackgasse mündet. Man könnte nun versuchen, den Parameter z kleiner zu wählen, so daß das Hauptglied Oberhand gegenüber dem Restterm gewinnt[24]. Bestenfalls bekommt man hier aber das Ergebnis

$$\pi_d(N+d) < c\frac{N}{\log\log N}$$

was aber trivial ist, da man selbst für die Anzahl aller Primzahlen (und nicht nur d-Zwillinge) eine bessere Schranke kennt[25]:

$$c_1\frac{N}{\log N} < \pi(N) < c_2\frac{N}{\log N}. \tag{1.14}$$

Lange Zeit glaubte man, die hier vorgestellte Siebmethode sei für das Finden guter oberer und unterer Schranken (geschweige denn asymptotischer Formeln) wegen der oben angeführten Probleme einfach nicht mächtig genug. Doch 1919 gelang es Viggo Brun mit einer Verbesserung dieser Methode Fortschritte zu machen. Bevor wir diese im nächsten Abschnitt vorstellen, holen wir noch den Beweis des Lemmas 1.4.3 nach, das vielerorts nur für die 2-Zwillinge bewiesen wird, hier aber ein bißchen allgemeiner gefaßt wird und uns auch im 2. Kapitel nützlich sein wird.

Lemma 1.4.3 *Seien $b, d, y \in \mathbb{N}$ konstant, $z \geq 2$, $b < y$ und $\mathcal{P} := \{p \in \mathbb{P}_d,\ y \leq p \leq z\}$. Dann gibt es eine nur von b, d und y abhängige Konstante B, so daß für $z \to \infty$ gilt*

$$\prod_{p\in\mathcal{P}}\left(1-\frac{b}{p}\right) = e^{B+o(1)}\frac{1}{\log^b z}. \tag{1.15}$$

---

[23] vgl. z.B Prachar [31] S. 19

[24] Übrigens ein erfolgsbringender Trick im anderen Zusammenhang bei der Anwendung auf $\pi(z)$, obwohl auch dort das Ergebnis zwar schwach, aber brauchbar ist. vgl z.B. Schwarz [34] S.16ff

[25] vgl. z.B. Prachar [31] S. 19. Das Ergebnis selbst stammt von Tchebyscheff [39]

Beweis: Durch Logarithmieren des Produkts erhalten wir

$$\begin{aligned}\log\prod_{p\in\mathcal{P}}\left(1-\frac{b}{p}\right) &= \log\underbrace{\prod_{\substack{p|d\\p\geq y}}\left(1-\frac{b}{p}\right)^{-1}\prod_{y\leq p\leq z}}_{=:D}\left(1-\frac{b}{p}\right)\\ &= \sum_{y\leq p\leq z}\left(\log\left(1-\frac{b}{p}\right)+\frac{b}{p}\right)-b\sum_{y\leq p\leq z}\frac{1}{p}+\log D\end{aligned}$$

mit der implizit definierten Konstanten $D>0$. Weiter gilt für die Logarithmusreihe $\ln(1+x) = -\sum_{n=1}^{\infty}(-x)^n/n$ für alle $|x|<1$. Damit gilt für alle $b<y\leq p$:

$$\begin{aligned}\left|\log\left(1-\frac{b}{p}\right)+\frac{b}{p}\right| &= \left|-\sum_{n=2}^{\infty}\frac{b^n}{np^n}\right|\\ &< \frac{1}{2}\sum_{n=2}^{\infty}\left(\frac{b}{p}\right)^n = \frac{1}{2}\left(\sum_{n=0}^{\infty}\left(\frac{b}{p}\right)^n-1-\frac{b}{p}\right)\\ &= \frac{b^2}{2p(p-b)}.\end{aligned}$$

Deshalb konvergiert für $z\to\infty$ die Reihe

$$\begin{aligned}\sum_{y\leq p\leq z}\left|\log\left(1-\frac{b}{p}\right)+\frac{b}{p}\right| &< \sum_{y\leq p\leq z}\frac{b^2}{2p(p-b)}\\ &< \frac{b^2}{2}\sum_{n\geq y}\frac{1}{(n-b)^2}\\ &\leq \frac{b^2}{2}\sum_{n\geq b+1}\frac{1}{(n-b)^2} = \frac{\pi^2b^2}{12}.\end{aligned}$$

Aus der elementaren Zahlentheorie kennt man das Ergebnis[26]

$$\sum_{y\leq p\leq z}\frac{1}{p} = \log\log z+\gamma+\mathcal{O}\left(\frac{1}{\log z}\right),\qquad z\to\infty \tag{1.16}$$

[26] vgl. etwa Krätzel [26] S.109ff.

mit einer geeigneten von y abhängigen Konstanten[27]

$$\gamma := 0,577215665\ldots - \sum_{2\le p<y} \frac{1}{p} + \underbrace{\sum_{p}(\log(1-1/p)+1/p)}_{|\cdot|\le\pi^2/12}.$$

Damit folgt schließlich für $z \to \infty$:

$$\log \prod_{p\in\mathcal{P}} \left(1-\frac{b}{p}\right) \quad = \quad -b\log\log z + B + o\,(1)\,.$$

mit einer noch näher zu spezifizierenden Konstanten

$$B \in \left[\log D - b\gamma - \frac{\pi^2 b^2}{12}, \log D - b\gamma + \frac{\pi^2 b^2}{12}\right],$$

die numerisch für verschiedene Wahlen der Parameter berechenbar ist.

$\square$

1.5 Das kombinatorische Sieb von Brun

So wie es unbewiesene Vermutungen gibt, gibt es auch Sätze in der Mathematik mit mehr als einem Beweis. Einer davon ist der Satz über die Unendlichkeit der Primzahlmenge[28]. Eine Möglichkeit für diesen Beweis ist der 1748 von Euler gefundene Nachweis[29], daß die Reihe

$$\sum_{p} \frac{1}{p}$$

erstreckt über alle Primzahlen divergiert, was natürlich auch viel mehr als nur die Unendlichkeit der Primzahlmenge bestätigt[30]. Wie dem auch sei, Euler war der erste, der analytische Methoden auf zahlentheoretische Probleme

[27] vgl. z.B. Hardy, Wright [22] S.399

[28] Sechs verschiedene Beweise kann der Leser z.B. in Aigner, Ziegler [1] Kap.1 finden.

[29] vgl. Euler [16]

[30] Zum Beispiel folgt daraus, daß Primzahlen häufiger als Quadratzahlen sind.

anwendete - ein Novum im 18. Jahrhundert, das bald darauf Schule machte. Es lag nun nahe, Ähnliches mit der Reihe

$$\sum_{p \text{ Zwilling}} \frac{1}{p}$$

zu versuchen, aber es funktionierte nicht.

Viggo Brun zeigte nun den folgenden bemerkenswerten[31]

Satz 1.5.1 *Auch wenn es unendlich viele Primzahlen p gibt, so daß $p+2$ Primzahl ist*[32]*, hat die über jene p erstreckte Summe*

$$\sum_{p \text{ Zwilling}} \frac{1}{p} = \frac{1}{3} + \frac{1}{5} + \frac{1}{11} + \frac{1}{17} + \frac{1}{29} + \cdots \tag{1.17}$$

einen endlichen Wert.

Bemerkung 1: Die Konvergenz der Reihe (1.17) hat also zur Folge, daß man wieder nichts über die Unendlichkeit der Menge der 2-Zwillinge erfährt. Verglichen mit dem Eulerschen Ergebnis weiß man nun aber, daß es viel mehr Primzahlen als 2-Zwillinge geben muß.
Bemerkung 2: Wegen $\frac{2}{p} > \frac{1}{p} + \frac{1}{p+2} > \frac{1}{p}$ ändert sich nichts am Konvergenzverhalten der Reihe, wenn man in die Summe (1.17) die Primzahlen $p+2$ mit aufnimmt: $\frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \frac{1}{19} + \frac{1}{29} + \frac{1}{31} + \cdots$.

V. Brun hatte die Summe (1.5) studiert und wollte wissen, wie sich ihr Wert verändert, wenn man nur über Teiler t summiert, deren Primteileranzahl $\omega(t)$ eine gewisse Zahl m nicht überschreitet. Das Ergebnis gibt das folgende Lemma[33]:

Lemma 1.5.1 *Für alle $k \in \mathbb{N}$ und alle $0 \leq m \leq \omega(k)$ gilt*

$$\sum_{\substack{t|k \\ \omega(t)\leq m}} \mu(t) \begin{cases} = 1, & \textit{falls } k = 1, \\ \geq 0, & \textit{falls } k > 1 \textit{ und } m \textit{ gerade ist,} \\ \leq 0, & \textit{falls } k > 1 \textit{ und } m \textit{ ungerade ist.} \end{cases} \tag{1.18}$$

[31] vgl. Brun [6]
[32] in unserer Namensgebung handelt sich hierbei um die 2-Zwillinge
[33] vgl. auch [35] S.40 oder [28] S.71ff

Beweis: Analog wie schon im Zusammenhang mit der Gleichung (1.5) argumentiert man kombinatorisch und findet sogar eine genaue Formel für die Summe (1.18):

$$\sum_{\substack{t|k \\ \omega(t)\leq m}} \mu(t) = \sum_{j=0}^{m}(-1)^j\binom{\omega(k)}{j} = (-1)^m\binom{\omega(k)-1}{m}.$$

Die letzte Gleichung kann man leicht induktiv beweisen. Die auftauchenden Binomialkoeffizienten sind stets positiv[34] und mit dem Vorfaktor $(-1)^m$ folgt die Behauptung.

□

Bemerkung 1: Der Vergleich von (1.18) mit (1.5) ergibt nun unmittelbar, daß uns mit dem Lemma 1.5.1 eine Möglichkeit zugespielt worden ist, untere und obere Schranken für Siebe der Form (1.6) zu erhalten. Falls wir alle Bezeichnungen des Abschnitts 1.4 übernehmen, dann folgt aus dem Lemma 1.3.1 und der Gleichung (1.7)

$$S(N) = \sum_{t|P(z)} \mu(t) \sum_{k\in\mathcal{K}_t} 1 = \sum_{n=1}^{N} \sum_{t|\,\mathrm{ggT}(h(n),P(z))} \mu(t). \tag{1.19}$$

Die innere Summe in (1.19) ist nach Lemma 1.3.1 gleich 1, falls $h(n)$ und $P(z)$ teilerfremd sind und ansonsten gleich 0. Nach dem Lemma 1.5.1 ergibt sich nun

$$S(N) \leq \sum_{n=1}^{N} \sum_{\substack{t|\,\mathrm{ggT}(h(n),P(z)) \\ \omega(t)\leq m,\ m\ gerade}} \mu(t) \tag{1.20}$$

$$\geq \sum_{n=1}^{N} \sum_{\substack{t|\,\mathrm{ggT}(h(n),P(z)) \\ \omega(t)\leq m,\ m\ ungerade}} \mu(t). \tag{1.21}$$

Bemerkung 2: Die untere Schranke in (1.21) bringt weitere Schwierigkeiten mit sich, da die Anzahl der Fälle mit $\mathrm{ggT}(h(n), P(z)) > 1$ normalerweise sehr viel größer ist als der mit $\mathrm{ggT}(h(n), P(z)) = 1$, so daß die Summe insgesamt

[34] eigentlich nur, wenn $\omega(k) > 0$ ist, aber im Falle $\omega(k) = 0$ ist $k = 1$ und dort ist nichts zu zeigen.

schnell ≤ 0 werden kann. Dann aber erhalten wir wegen $S(N) \geq 0$ nur eine triviale untere Schranke.

Als nächstes definieren wir die sog. elementarsymmetrischen Funktionen[35], die wir für den Rest des Textes mit $\Sigma_1, \ldots, \Sigma_\rho$ beizeichnen. Wir werden auf sie auch im 2. Kapitel zurückkommen.

Definition 1.5.1 *Seien $\xi_1, \ldots, \xi_\rho$ beliebige komplexe Zahlen. Multipliziert man das Polynom*

8150

$$p(x) := (x + \xi_1) \cdots (x + \xi_\rho)$$

aus, dann kann man auch

$$p(x) = x^\rho + \Sigma_1 x^{\rho-1} + \cdots + \Sigma_{\rho-1} x + \Sigma_\rho$$

schreiben mit den ***elementarsymmetrischen Funktionen*** $\Sigma_r : \mathbb{C}^\rho \to \mathbb{C}$, *$r = 1, \ldots, \rho$, die definiert sind wie folgt:*

$$\begin{aligned}
\Sigma_1(\xi_1, \ldots, \xi_\rho) &= \sum_{1 \leq r \leq \rho} \xi_r \\
\Sigma_2(\xi_1, \ldots, \xi_\rho) &= \sum_{1 \leq r < s \leq \rho} \xi_r \xi_s \\
\Sigma_3(\xi_1, \ldots, \xi_\rho) &= \sum_{1 \leq r < s < t \leq \rho} \xi_r \xi_s \xi_t \\
&\vdots \\
\Sigma_\rho(\xi_1, \ldots, \xi_\rho) &= \xi_1 \cdots \xi_\rho
\end{aligned}$$

Bemerkung: Wie man sieht, haben die elementarsymmetrischen Funktionen einige interessante kombinatorische Eigenschaften. Salopp gesprochen stellt Σ_r die Summe über genau $\binom{\rho}{r}$ Summanden dar, die alle Produktkombinationen von r Faktoren aus ρ möglichen Faktoren durchlaufen. Im 2. Kapitel werden wir davon Gebrauch machen und eine komplizierte Summe über viele Σ_r einfach als Wert des Polynoms $p(x)$ für bestimmte Argumente x ausdrücken.

Für den gleich vorgestellten Brunschen Satz werden wir die folgende Eigenschaft der Σ_r ausnützen:

---

[35] vgl. z.B. Schwarz [35] S. 46

Lemma 1.5.2 *Für alle r mit $1 \leq r \leq \rho$ gilt die Abschätzung*

$$\Sigma_r(\xi_1, \ldots, \xi_\rho) \leq \frac{(\Sigma_1(\xi_1, \ldots, \xi_\rho))^r}{r!} \tag{1.22}$$

für beliebige (reelle) Zahlen $\xi_1, \ldots, \xi_\rho > 0$.

Beweis: (z.B. Schwarz [35]) Die Polynomialentwicklung von $(\Sigma_1)^r$ ergibt nämlich

$$\begin{aligned}(\Sigma_1)^r &= (\xi_1 + \cdots + \xi_\rho)^r = \sum_{\substack{n_1+\cdots+n_\rho=r \\ 0\leq n_j}} r! \frac{\xi_1^{n_1} \cdots \xi_\rho^{n_\rho}}{n_1! \cdots n_\rho!} \\ &\geq \sum_{\substack{n_1+\cdots+n_\rho=r \\ 0\leq n_j \leq 1}} r! \frac{\xi_1^{n_1} \cdots \xi_\rho^{n_\rho}}{n_1! \cdots n_\rho!} = r!\ \Sigma_r.\end{aligned}$$

□

In der dem Verfasser vorliegenden Literatur zu diesem Thema[36] findet man den folgenden Satz nur für $d = 2$ nachgerechnet, da man dort vielleicht bestrebt war, das Brunsche Ergebnis historisch wiederzugeben. Nichts spricht aber dagegen, den Brunschen Satz auf alle geraden $d \geq 2$ auszudehnen, was im folgenden geschehen soll.

Satz 1.5.2 *Sei $d \geq 2$ gerade. Dann existiert eine von d abhängige Konstante C_d, mit der für $N \to \infty$ gilt:*

$$\pi_d(N) \leq C_d \frac{N}{\log^2 N} (\log\log N)^2. \tag{1.23}$$

Bemerkung: Es stellt sich später im Zusammenhang mit der Selbergschen Siebmethode heraus, daß man den Faktor $\log\log N^2$ weglassen kann. Während jedoch die vorigen Ergebnisse hoffnungslos waren, konnte Brun mit einfachen aber entscheidenden Verbesserungen dieses erstaunliche Resultat erzielen.
Beweis: Im folgenden bezeichnen C_d, C_d^1, $C_d^2, \ldots$ von d abhängige Konstanten. Wie im Abschnitt 1.4 sei $P(z) := \prod_{2\leq p\leq z} p$ (erstreckt über alle Primzahlen) und die Werte des Polynoms $h(n) = n(n+d)$ für $n = 1, \ldots, N$ gegeben. Wir bezeichnen wieder mit $\beta(t)$ die Anzahl der Kongruenzlösungen

[36] Schwarz [35] S.41 ff, Halberstam&Richert [19] S.51, Landau [28] Kap.2

von $h(n) \equiv 0(t)$ für $n = 1, \ldots, t$; mit $\mathbb{P}_d$ alle Primzahlen, die d nicht teilen und setzen

$$S(N) = \#\{\mathrm{ggT}(h(n), P(z)) = 1,\ n = 1, \ldots, N\}.$$

Nach (1.20), (1.7) und dem Lemma 1.4.1 gilt dann für gerade $m \geq 2$:

$$\begin{aligned}
S(N) &\leq \sum_{n=1}^{N} \sum_{\substack{t \mid \mathrm{ggT}(h(n),P(z)) \\ \omega(t) \leq m}} \mu(t) \\
&= \sum_{\substack{t \mid P(z) \\ \omega(t) \leq m}} \mu(t) \sum_{h(n) \equiv 0 \bmod t} 1 \\
&= \underbrace{N \sum_{\substack{t \mid P(z) \\ \omega(t) \leq m}} \mu(t) \frac{\beta(t)}{t}}_{=:Z_1(N)} + \mathcal{O}\left(\sum_{\substack{t \mid P(z) \\ \omega(t) \leq m}} \mu(t) R_t \right).
\end{aligned}$$

Vergleicht man nun die letzte Gleichung mit (1.8), so sieht man, daß der Trick von Brun darin bestand, die Summe über die Teiler $t|P(z)$ so zu modifizieren, daß man ihre Anzahl im Fehlerterm drastisch reduziert und trotzdem noch eine obere Schranke bekommt. Für das Hauptglied $Z_1(N)$ erhält man analog zu (1.11) mit derselben Konstanten C_d

$$Z_1(N) = C_d N \cdot \prod_{\substack{2 \leq p \leq z \\ p \in \mathbb{P}_d}} \left(1 - \frac{2}{p}\right) - \underbrace{N \sum_{\substack{t \mid P(z) \\ \omega(t) > m}} \mu(t) \frac{\beta(t)}{t}}_{=:Z_2(N)}.$$

Nach Lemma 1.4.3 gilt für das Produkt für $b = 2$, $d \geq 2$ gerade und $N, z \to \infty$ mit einer neuen Konstanten C_d^1

$$C_d N \cdot \prod_{\substack{2 \leq p \leq z \\ p \in \mathbb{P}_d}} \left(1 - \frac{2}{p}\right) = C_d^1 \frac{N}{\log^2 z}.$$

Nach (1.9) und dem Lemma 1.4.2 gilt nun

$$Z_2(N) = N \sum_{\substack{t \mid P(z) \\ \omega(t) > m}} \mu(t) \frac{2^{h_t}}{t}.$$

Dabei bezeichnen die h_t die Anzahlen derjenigen Primfaktoren von t, die d nicht teilen, in anderen Worten ist $h_t := \omega(t/\operatorname{ggT}(t,d))$. Übrigens sind alle t als Teiler von $P(z)$ quadratfreie Zahlen. Es gilt $h_t = 0$, wenn $\operatorname{ggT}(t,d) = t$ und $h_t = \omega(t)$, wenn wenn $\operatorname{ggT}(t,d) = 1$. Werte zwischen 0 und $\omega(t)$ werden angenommen, wenn $t \nmid d$ aber $\operatorname{ggT}(t,d) > 1$ ist. Wiederholen wir die letzte Rechnung im Betrag, dann machen wir die zweite Summe nur größer, wenn wir statt der Exponenten h_t die Exponenten $\omega(t)$ nehmen, die ja alle $> m$ sind. Damit folgt

$$|Z_2(N)| \;\le\; N \sum_{r=m+1}^{\rho} 2^r \sum_{\substack{t\mid P(z)\\ \omega(t)=r}} \frac{1}{t}.$$

Dabei ist die Zahl ρ dadurch definiert, daß $p_\rho = \operatorname{gPf}(P(z))$ den größten Primfaktor von $P(z)$ darstellt. Setzen wir noch $p_1 = 2$, dann finden wir die Beziehung

$$\sum_{\substack{t\mid P(z)\\ \omega(t)=r}} \frac{1}{t} = \Sigma_r\left(\frac{1}{p_1}, \ldots, \frac{1}{p_\rho}\right), \tag{1.24}$$

wobei Σ_r die r-te elementarsymmetrische Funktion der Primzahlkehrwerte $\frac{1}{p_1}, \ldots, \frac{1}{p_\rho}$ ist. Mit dem Ergebnis (1.16) für $b = 1$ erhalten wir mit einer geeigneten Konstanten c weiter $\Sigma_1(\frac{1}{p_1}, \ldots, \frac{1}{p_\rho}) \le c \log\log z$, so daß wir mit dem Lemma 1.5.2 die Abschätzung

$$\sum_{\substack{t\mid P(z)\\ \omega(t)=r}} \frac{1}{t} \le \frac{(c\log\log z)^r}{r!} \le \left(\frac{c\log\log z}{r}\right)^r \tag{1.25}$$

erhalten. Damit folgt

$$|Z_2(N)| \;\le\; N \sum_{r=m+1}^{\rho} \left(\frac{2c\log\log z}{r}\right)^r < N \sum_{r=m+1}^{\infty} \left(\frac{2c\log\log z}{r}\right)^r.$$

Setzen wir nun

$$\frac{m+1}{2} < 2c\log\log z < m+1 \tag{1.26}$$

voraus, dann sind alle Summanden echt kleiner als 1 aber größer als 1/2 und es folgt

$$|Z_2(N)| \;\le\; N \sum_{r=m+1}^{\infty} \frac{1}{2^r} = \frac{N}{2^m}.$$

Nun müssen wir uns noch um den Restterm

$$\mathcal{O}\left(\sum_{\substack{t|P(z)\\ \omega(t)\leq m}} \mu(t)R_t\right)$$

kümmern. Hier gilt wegen $R_t \leq \beta(t)$

$$\begin{aligned}
\left|\sum_{\substack{t|P(z)\\ \omega(t)\leq m}} \mu(t)R_t\right| &\leq \sum_{\substack{t|P(z)\\ \omega(t)\leq m}} \beta(t) \\
&\leq \sum_{r=0}^{m} 2^r \binom{\rho}{r} \\
&\leq 2^m \sum_{r=0}^{m} \rho^r \leq (2\rho)^m.
\end{aligned}$$

Bemerkung: Im zweiten Schritt steht das Zeichen $\leq$ und nicht $=$, weil nicht alle Teiler $t|P(z)$ unter den $\binom{\rho}{r}$ vielen mit $\omega(t) = r$ den größten Wert $\beta(t) = 2^r$ erreichen. Hier müßte eigentlich mit der obigen Bezeichnung $\beta(t) = 2^{h_t}$ mit $0 \leq h_t \leq r$ stehen.
Damit erhalten wir insgesamt

$$S(N) \leq C_d^1 \frac{N}{\log^2 z} + N\frac{1}{2^m} + (2\rho)^m$$

und somit

$$\pi_d(N) \leq C_d^2\rho + C_d^1 \frac{N}{\log^2 z} + N\frac{1}{2^m} + (2\rho)^m \tag{1.27}$$

Nun muß z so groß sein, daß wir $2 < \rho \leq z$ wählen können und (1.26) mit einem m erfüllt ist. Für genügend großes N sind diese Bedingungen für

$$z = N^{1/3c\log\log N} \text{ und } m = \lfloor 2c\log\log N \rfloor$$

erfüllt, denn dann ist

$$\frac{2c\log\log N}{2} < 2c\log\log z = 2c(\log\log N - \log(3c\log\log N)) < 2c\log\log N.$$

Setzen wir es in (1.27) ein, so erhält man

$$\begin{aligned}\pi_d(N) \quad &\le \quad C_d^3 \left\{ \rho + \frac{N(\log\log N)^2}{\log^2 N} \right. \\ &\left. + \frac{N}{2^{\lfloor 2c \log\log N \rfloor}} + (2\rho)^{\lfloor 2c\log\log N\rfloor} \right\}. \end{aligned} \tag{1.28}$$

Nun existiert nach (1.14) eine weitere Konstante c', so daß höchstens

$$\rho = \pi(z) \le c' \frac{N^{1/3c\log\log N} 3c \log\log N}{\log N}$$

gilt. Damit könnte nur der letzte Summand in (1.28) Schwierigkeiten bereiten, es ist aber

$$\begin{aligned}(2\rho)^m \quad &\le \quad (2\rho)^{2c\log\log N} \\ &\le \quad \exp\left(2c\log\log N \left\{ \log 2 + \log(c' 3c \log\log N) \right.\right. \\ &\qquad \left.\left. - \log\log N + \frac{\log N}{3c\log\log N} \right\}\right) \\ &\le \quad c'' \exp(\frac{2}{3}\log N) = c'' N^{2/3}.\end{aligned}$$

Also setzt sich der zweite Summand in (1.28) für $N \to \infty$ durch und daraus folgt die Behauptung.

□

Mit dem Satz 1.5.2 gelingt uns nun leicht der Beweis des folgenden Satzes, der eine Verallgemeinerung des Brunschen Satzes 1.5.1 ist.

Satz 1.5.3 *Auch wenn es unendlich viele d-Zwillinge gibt, sind die Summen*

$$\sum_{p \text{ ist } d-Zwilling} \frac{1}{p} \tag{1.29}$$

konvergent für alle geraden $d \ge 2$.

Beweis: Nach Satz 1.5.2 gibt es für genügend große N Konstanten C_d mit

$$\pi_d(N) < C_d \frac{N}{\log^{3/2} N}$$

Ist nun p_r die r-te Primzahl[37] mit der Eigenschaft, daß auch $p_r + d$ prim ist, dann gilt für alle $r \geq 1$:

$$r = \pi_d(p_r) < C_d \frac{p_r}{\log^{3/2} p_r} < C'_d \frac{p_r}{\log^{3/2} r}$$

also ist $\frac{C'_d}{r \log^{3/2} r} > \frac{1}{p_r}$ und damit

$$\sum_{p \text{ ist } d\text{-Zwilling}} \frac{1}{p} = \sum_{r=1}^{\infty} \frac{1}{p_r} < \sum_{r=1}^{\infty} \frac{C'_d}{r \log^{3/2} r} < \infty.$$

□

Halberstam und Richert waren der Meinung, daß die Brunsche Siebmethode in ihren Möglichkeiten noch nicht voll ausgeschöpft worden sei. Besonders ihr ausgeprägter kombinatorischer Charakter, auf den wir hier nicht weiter eingegangen sind, wirke, so die beiden Autoren, wegen seiner Kompliziertheit eher abschreckend für eine genauere Untersuchung, so daß nur wenige Spezialisten dieser Methode die gebührende volle Aufmerksamkeit schenkten, um überhaupt ihre ganze Tragweite zu erkennen[38]. Sie belegten dies damit, daß Hardy nach nur einmaliger Anwendung der Brunschen Siebmethode die Bemerkung machte, das Brunsche Sieb sei nicht mächtig oder profund genug, um das Goldbachsche Problem zu lösen. Ebenso schenkte Landau zunächst jahrelang der Brunschen Methode keine Beachtung, bis er ihre Vorzüge erst durch die Arbeiten Schnirelmanns erkannte. Barkeley Rosser entdeckte eine wichtige Verbesserung dieser Methode, doch seine Arbeit blieb zunächst für 20 Jahre unveröffentlicht.

Es könnte sein, daß durch die Fortschritte in der Kombinatorik des 20. Jahrhunderts bereits unentdeckte Wege existieren, die Möglichkeiten des Brunschen Siebs weiter auszubauen, was sicherlich eine reizvolle Forschungsrichtung darstellt. Einige weiterführende Anmerkungen zum Brunschen Sieb und den Arbeiten Rosser's findet man in Halberstam, Richert [19] Kap. 2. Die Darstellung der Selbergschen Siebtheorie für obere Schranken im nächsten Abschnitt wurde ebenfalls durch dieses Buch beeinflußt. Sie ist sehr allgemein und kann neben dem PZd-Problem auch auf eine Reihe anderer Siebprobleme angewandt werden. Mit der Selbergsche Siebmethode werden wir das Ergebnis des Satzes 1.5.2 vom Faktor $(\log \log N)^2$ befreien und so eine bessere obere Schranke für $\pi_d(N)$ finden.

[37] falls überhaupt unendlich viele solche existieren

[38] vgl. Halberstam, Richert [19] S. 6

1.6 Die Selbergsche Siebmethode für obere Schranken

Wie im Abschnitt 1.5 setzen wir im folgenden für $z \geq 2$

$$P(z) := \prod_{2 \leq p \leq z} p$$

und bezeichnen vorerst mit $\mathcal{P}$ eine unendliche Teilmenge aller Primzahlen $\mathbb{P}$, die wir nach der allgemeinen theoretischen Darstellung bei der Anwendung auf d-Zwillinge noch näher spezifizieren werden. Eine Menge $\mathcal{M}$ ganzer Zahlen heißt **teilergeschlossen**, falls mit $m \in \mathcal{M}$ auch alle Teiler $\mu | m$ in $\mathcal{M}$ liegen. Mit $\mathcal{P}^* \subseteq \mathbb{N}$ bezeichnen wir nun eine Menge bestehend aus allen aus den Primzahlen $p \in \mathcal{P}$ konstruierbaren Produkten und der Zahl 1. Das macht $\mathcal{P}^*$ zu einer teilergeschlossenen Menge.

Weiter denken wir uns vorerst $\mathcal{A}$ wieder als eine aus N verschiedenen positiven ganzen Zahlen $a_1, \ldots, a_N$ bestehende Menge.
Die Mengen $\mathcal{P}$ und $\mathcal{A}$ sollen ferner so zusammenhängen, daß für $N \to \infty$ fast alle $a \in \mathcal{A}$ eine Primzerlegung aus den Primzahlen $p \in \mathcal{P}$ besitzen und es umgekehrt keine Primzahl $p \in \mathcal{P}$ gibt, die kein $a \in \mathcal{A}$ teilt und keine Primzahl $p \in \mathbb{P}$ gibt, die alle $a \in \mathcal{A}$ teilt. In anderen Worten soll

$$\begin{aligned} &(a \in \mathcal{A} \implies a \in \mathcal{P}^*) \ \wedge \\ &(\forall p \in \mathcal{P}\ \exists a \in \mathcal{A}:\ p|a) \ \wedge \ (\nexists p \in \mathbb{P} : p|a\ \forall a \in \mathcal{A}) \end{aligned} \tag{1.30}$$

gelten bis auf nur endlich viele Ausnahmen für $N \to \infty$.

Ferner bezeichnen wir wieder für jedes $t \in \mathcal{P}^*$ mit $\mathcal{A}_t \subseteq \mathcal{A}$ diejenigen Teilmengen von $\mathcal{A}$, die nur Vielfache von t enthalten. Damit gilt speziell $\mathcal{A}_1 = \mathcal{A}$.

Wir nehmen nun an, daß es eine von $\mathcal{A}$ abhängige multiplikative Funktion $\beta : \mathbb{N} \to \mathbb{R}$ gibt, so daß für quadratfreie $t \in \mathcal{P}^*$ die "Fehlerterme"

$$R_t := \left| \frac{\beta(t)}{t} N - \#\mathcal{A}_t \right|, \qquad (\mu(t) \neq 0), \tag{1.31}$$

"klein" ausfallen. Die Forderung (1.30) können wir nun auch so formulieren:

Bedingung 1.6.1 *Für alle Primzahlen $p \in \mathbb{P}$ gelte*

$$0 \leq \frac{\beta(p)}{p} < 1$$

mit Gleichheit links ausschließlich für $p \in \mathbb{P} \backslash \mathcal{P}$

Der Bruch $\beta(p)/p$ sollte nämlich für alle $p \in \mathcal{P}$ echt größer als 0 sein, denn sonst müßte auch $\#\mathcal{A}_p$ fast 0 sein, wenn R_p klein ist, woraus folgt, daß p womöglich keine Zahl in $\mathcal{A}$ teilt und daher nicht siebend wirkt. Andererseits darf keine Primzahl $p \leq z$ für $z \to \infty$ alle oder fast alle $a \in \mathcal{A}$ teilen, denn dann sieben wir alle heraus (dies erklärt die rechte Ungleichung). Übrigens folgt aus dieser Bedingung auch $\beta(1) = 1$, weil β multiplikativ und nicht identisch Null ist. Denn wenn es mindestens ein m mit $\beta(m) \neq 0$ gibt, können wir wegen der Multiplikativität die Gleichung $\beta(1 \cdot m) = \beta(1) \cdot \beta(m)$ aufstellen und dann durch $\beta(m)$ durchdividieren, woraus diese Behauptung folgt.

Die Idee Selbergs beruht nun auf der folgenden Ungleichung. Seien $\lambda_1 = 1$ und für $t \geq 2$ beliebige reelle Zahlen λ_t gegeben. Dann gilt stets

$$S(\mathcal{A}, \mathcal{P}, z) \leq \sum_{a \in \mathcal{A}} \left(\sum_{t \mid \mathrm{ggT}(a, P(z))} \lambda_t \right)^2 ,$$

denn immer dann, wenn $\mathrm{ggT}(a, P(z)) = 1$ ist, taucht als einziger Teiler rechts $t = 1$ auf, wodurch das jeweilige $a \in \mathcal{A}$ genau einmal gezählt wird. In den Fällen mit $\mathrm{ggT}(a, P(z)) > 1$, die wir eigentlich nicht mitzählen wollen, ist das Quadrat der inneren Summe eine positive Zahl, da alle λ_t reell sind.

Nun besteht die ganze Kunst darin, die Zahlen λ_t so zu wählen, daß diese Ungleichung eine möglichst genaue obere Schranke liefert. Um das Problem zu präzisieren, vertauschen wir die Summationsreihenfolge und erhalten

$$S(\mathcal{A}, \mathcal{P}, z) \leq \sum_{\substack{t_\nu \mid P(z) \\ \nu = 1,2}} \lambda_{t_1} \lambda_{t_2} \sum_{\substack{a \in \mathcal{A} \\ a \equiv 0 \bmod \mathrm{kgV}(t_1, t_2)}} 1.$$

Setzen wir zur Abkürzung $T := \mathrm{kgV}(t_1, t_2)$, dann zählt die innere Summe genau die Größe $\#\mathcal{A}_T$, und es folgt mit unserer Forderung (1.31) die neue Abschätzung

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}, z) &\leq N \sum_{\substack{t_\nu \mid P(z) \\ \nu = 1,2}} \lambda_{t_1} \lambda_{t_2} \frac{\beta(T)}{T} + \sum_{\substack{t_\nu \mid P(z) \\ \nu = 1,2}} \lambda_{t_1} \lambda_{t_2} R_T \\ &=: N Z_1 + Z_2 \end{aligned} \tag{1.32}$$

Es stellt sich nun heraus, daß es sogar für sehr einfache Folgen $\mathcal{A}$ extrem schwierig ist, die λ_t für $t > 1$ so zu wählen, daß die Fehlersumme Z_2 minimal ausfällt. Selberg stellte an die Parameter λ die folgenden Bedingungen:

Bedingung 1.6.2 *Für alle $t \in \mathcal{P}^*$ mit $t > z$ wird $\lambda_t = 0$ gesetzt, um die Anzahl der Summanden in Z_2 zu reduzieren.*

Bedingung 1.6.3 *Für alle $t \in \mathcal{P}^*$ mit $2 \leq t \leq z$ sollen λ_t so gewählt werden, daß Z_1 minimal wird.*

Die Bedingung 1.6.2 liegt auf der Hand, denn alle t in der Summe haben zwar Primteiler $\leq z$, sind aber größtenteils selbst größer als z. Somit verschwinden für extrem viele T die Summanden in Z_2.
Diese Bedingung ist so einfach, daß sie fast schon trivial wirkt. Dennoch bestand die hohe Kunst Selbergs darin, ein technisches Regelwerk zu konstruieren, das später in der Lage ist, siebtheoretische Ergebnisse hervorzuzaubern, ohne die Konformität mit dieser banalen Bedingung einzubüßen und gleichzeitig noch die Bedingung 1.6.3 zu erfüllen. Dieses Regelwerk soll im Satz 1.6.1 vorgestellt werden.

Doch zunächst berichten wir über einige einfache Ergebnisse über multiplikative Funktionen, die wir für den Beweis des Satzes 1.6.1 brauchen werden und deren Beweise sich in fast jeder Einführung in die Zahlentheorie bzw. Siebtheorie finden lassen.

Lemma 1.6.1 *Für jede multiplikative Funktion f gilt*

$$f(t_1)f(t_2) = f(\mathrm{ggT}(t_1, t_2)) \cdot f(\mathrm{kgV}(t_1, t_2)).$$

Beweis: Vgl. Schwarz [35], S. 170.

□

Definition 1.6.1 *Seien $g, f : \mathbb{N} \to \mathbb{C}$ zwei arithmetische Funktionen. Die neue arithmetische Funktion*

$$h(n) := (g * f)(n) = \sum_{t|n} g(t) f\left(\frac{n}{t}\right) \qquad \forall\, n \in \mathbb{N}$$

*heiße **Faltung** von g und f und die Funktion*

$$i(n) := (g \cdot f)(n) = g(n)f(n), \qquad \forall\, n \in \mathbb{N}$$

*heiße **punktweises Produkt** von g und f.*

Lemma 1.6.2 (Faltung, punktweises Produkt und Multiplikativität)

1. *Sind f, g multiplikative Funktionen, so sind ihre Faltung $h = g * f$ und ihr punktweises Produkt $i = g \cdot f$ auch multiplikativ.*
2. ***Möbiussche Umkehrformel*** *Sei g eine arithmetische Funktion. Definiert man $f := 1 * g$, dann gilt $g = \mu * f$. Ist umgekehrt f eine arithmetische Funktion, und definiert man $g := \mu * f$, dann gilt $f = 1 * g$.*

Beweis: Die Beweise zu diesen und 6 weiteren nützlichen Aussagen über die Faltung befinden sich z.B. in Schwarz [35], S.14-19.

□

Wir bilden nun die Funktion $\gamma(t) := t/\beta(t)$ für alle $t \geq 1$, die nach Lemma 1.6.2/1 multiplikativ ist. Wegen der Bedingung 1.6.1 gilt also $1 < \gamma(t) \leq \infty$ für $t > 1$. $\gamma(t) = \infty$ soll hierbei bedeuten, daß $\beta(t) = 0$ ist, also daß t durch mindestens eine der Primzahlen $p \in \mathbb{P} \backslash \mathcal{P}$ teilbar ist. Dann ist allerdings $\# \mathcal{A}_t = 0$ und unser Sieb trivial. Damit können wir auch schreiben

$$Z_1 = \sum_{\substack{t_\nu | P(z) \\ \nu = 1,2}} \frac{\lambda_{t_1} \lambda_{t_2}}{\gamma(T)} \tag{1.33}$$

Selberg zeigte nun im Wesentlichen folgendes:

Satz 1.6.1 *Sei g eine Funktion definiert durch*

$$g(t) := \mu * \gamma = \sum_{\tau | t} \mu(t) \gamma\left(\frac{t}{\tau}\right). \tag{1.34}$$

Ferner sei für positive z

$$G_t(z) := \sum_{\substack{b < z \\ \mathrm{ggT}(b,t) = 1}} \frac{\mu^2(b)}{g(b)} \tag{1.35}$$

und speziell

$$G(z) := G_1(z) = \sum_{b \leq z} \frac{\mu^2(b)}{g(b)}.$$

Setzt man nun

$$\lambda_t = \frac{\mu(t)}{\prod_{p|t}(1-1/\gamma(p))} \frac{G_t(z/t)}{G(z)}, \tag{1.36}$$

dann gilt $\lambda_1 = 1$, *die Bedingungen 1.6.2 und 1.6.3 sind erfüllt, und es gilt die obere Abschätzung*

$$S(\mathcal{A}, \mathcal{P}, z) \;\leq\; \frac{N}{G(z)} + \sum_{\substack{t_\nu < z \\ \nu=1,2}} \lambda_{t_1}\lambda_{t_2} R_T \tag{1.37}$$

Beweis: Zunächst bemerken wir, daß wegen $\gamma(p) > 1$ die Funktion g für alle $t \in \mathcal{P}^*$ wohldefiniert ist (für $t \notin \mathcal{P}^*$ gilt $g(t) = \infty$). Wegen des Faktors $\mu^2(b)$ läuft die Summe $G_t(z)$ nur über quadratfreie $b \leq z$. g ist als Faltung von μ und γ selbst multiplikativ (Lemma 1.6.2.1). Für quadratfreie b gilt also

$$g(b) = \gamma(b) \prod_{p|b} \left(1 - \frac{1}{\gamma(p)}\right) \tag{1.38}$$

Deshalb ist g nicht identisch 0 und deshalb gilt $g(1) = 1$. Damit folgt also, daß stets $G(z) \geq 1$ ist, weil g überall sonst positiv ist.

Für $t = 1$ erhalten wir, wie man sieht, $\lambda_1 = 1$. Ferner verschwinden alle λ_t, falls t nicht quadratfrei ist, aber nicht nur diese: Für $t > z$ ist die Summe $G_t(z/t)$ leer also Null. Dort gilt somit $\lambda_t = 0$, wie verlangt.

Damit haben wir bereits $\lambda_1 = 1$ mit der Bedingung 1.6.2 bewiesen und den Summationsindex in (1.37) erklärt. Wir sehen nun auch den enormen Fortschritt bei unserem Hauptproblem - der Anzahl der Summanden in Z_2. Die Summe in (1.37) hat nur z^2 Glieder, während die Summe Z_2 in (1.32) noch $2^{\pi(z)} > 2^{cz/\log z}$ Summanden enthielt.

Die Bedingung 1.6.3 folgt zusammen mit der Ungleichung (1.37), wenn wir zeigen können, daß Z_1 bei

$$\frac{1}{G(z)}$$

sein Minimum findet. Zunächst tun wir so, als ob wir von der Formel (1.36) für die λ_t nichts wüßten und werden versuchen, das Minimum von Z_1 zunächst unabhängig vom Wert der λ_t zu finden. Dabei wird die Formel (1.36) als Nebenprodukt herauskommen. Wegen dem Lemma 1.6.1 erhalten wir zunächst

$$\begin{aligned} Z_1 &= \sum_{\substack{t_\nu \mid P(z) \\ \nu=1,2}} \frac{\lambda_{t_1}\lambda_{t_2}}{\gamma(T)} = \sum_{\substack{t_\nu \mid P(z) \\ \nu=1,2}} \lambda_{t_1}\lambda_{t_2} \frac{\gamma(\mathrm{ggT}(t_1,t_2))}{\gamma(t_1)\gamma(t_2)} \\ &= \sum_{\substack{t_\nu \mid P(z) \\ \nu=1,2}} \frac{\lambda_{t_1}\lambda_{t_2}}{\gamma(t_1)\gamma(t_2)} \sum_{b \mid \mathrm{ggT}(t_1,t_2)} g(b), \end{aligned}$$

da nach dem Lemma 1.6.2/2 $\gamma = 1 * g$ gilt. Die Vertauschung der Summationsreihenfolge liefert

$$Z_1 = \sum_{b \mid P(z)} g(b) \sum_{\substack{t_\nu \mid P(z),\ \nu=1,2 \\ b \mid t_1, b \mid t_2}} \frac{\lambda_{t_1}\lambda_{t_2}}{\gamma(t_1)\gamma(t_2)}.$$

Dies bedarf einer kurzen Erläuterung. Da wir nun in der äußeren Summe über alle Teiler $b|P(z)$ und in der inneren über alle Paare $t_1|P(z)$ und $t_2|P(z)$ summieren, müssen wir den Summationsindex der inneren Summe insofern einschränken, daß wir nur die Paare treffen, bei denen $b|\,\mathrm{ggT}(t_1,t_2)$ gilt. Notwendig und hinreichend dafür ist, daß $b|t_1$ und $b|t_2$.

Aufgrund unserer Bedingung 1.6.2 verschwindet die innere Summe immer dann, wenn $t_1 > z$ oder $t_2 > z$. Soll nun b beide Zahlen teilen, kann es in den nicht verschwindenden Termen also auch nur echt $\leq z$ sein, und es muß quadratfrei sein, denn die t_ν sind als Teiler von $P(z)$ quadratfrei. Da nun aber alle quadratfreien Zahlen $b \leq z$ automatisch Teiler von $P(z)$ sein müssen, können wir die Summationsindex $b|P(z)$ durch den Summationsindex $b \leq z$ ersetzen, denn die Bedingung $b|t_\nu$ in der inneren Summe sorgt schon für die Quadratfreiheit von b. Nach diesen Bemerkungen ist die nächste Umformung leicht verständlich:

$$\begin{aligned} Z_1 &= \sum_{b \leq z} g(b) \left(\sum_{\substack{t \leq z \\ b|t}} \frac{\lambda_t}{\gamma(t)} \right)^2 \\ &=: \sum_{b \leq z} g(b)\eta_b^2(z), \end{aligned} \tag{1.39}$$

mit der Funktion

$$\eta_b(z) := \sum_{\substack{t \le z \\ b|t}} \frac{\lambda_t}{\gamma(t)} = \sum_{r \le z/b} \frac{\lambda_{br}}{\gamma(br)}. \tag{1.40}$$

Nun gilt aber stets

$$\eta_b(z) = \sum_{n \le z/b} \eta_{bn}(z) \sum_{k|n} \mu(k) = \sum_{r \le z/b} \sum_{k \le z/(br)} \mu(k)\eta_{brk}(z), \tag{1.41}$$

so daß der Indexvergleich von (1.41) mit (1.40) die Beziehung

$$\frac{\lambda_t}{\gamma(t)} = \sum_{k \le z/t} \mu(k)\eta_{tk}(z) \tag{1.42}$$

liefert.

Unsere Aufgabe ist nun, herauszufinden, wo das Minimum der quadratischen Form der reellen Zahlen $\eta_b(z)$

$$Z_1(\eta_b(z)) = \sum_{b \le z} g(b)(\eta_b(z))^2$$

angenommen wird mit der Nebenbedingung $\lambda_1 = 1$ also nach (1.42)

$$Y_1(\eta_b(z)) = \sum_{b \le z} \mu(b)\eta_b(z) = \frac{\lambda_1}{\gamma(1)} = 1.$$

Als notwendige Bedingungen für ein Extremum muß das Gleichungssystem

$$\frac{\partial Z_1}{\partial \eta_b(z)} + \alpha \frac{\partial Y_1}{\partial \eta_b(z)} = 0, \qquad b = 1, \ldots, \lfloor z \rfloor$$

erfüllt sein mit einem noch unbekannten Multiplikator α. Dieses Gleichungssystem ergibt

$$2g(b)\eta_b(z) + \alpha\mu(b) = 0, \qquad b = 1, \ldots, \lfloor z \rfloor.$$

Wenn b quadratfrei ist, folgt wegen (1.38) also $g(b) \neq 0$ und man findet dort

$$\eta_b(z) = -\frac{\alpha\mu(b)}{2g(b)}, \qquad b = 1, \ldots, \lfloor z \rfloor. \tag{1.43}$$

Die Nebenbedingung ergibt damit

$$1 = -\frac{\alpha}{2}\sum_{b\le z}\frac{\mu^2(b)}{g(b)} \iff \alpha = -\frac{2}{G(z)}.$$

Setzt man dies in (1.43) ein, ergibt sich

$$\eta_b(z) = \frac{\mu(b)}{g(b)}\cdot\frac{1}{G(z)}, \qquad b = 1,\ldots,\lfloor z\rfloor \tag{1.44}$$

als notwendige Bedingung für ein Extremum in Z_1. Dieses kann also nur bei

$$Z_1 = \sum_{b\le z}\frac{\mu^2(b)}{g(b)}\left(\frac{1}{G(z)}\right)^2 = \frac{1}{G(z)}$$

liegen. Es kann aber nur ein Minimum sein, denn die Ungleichung (1.32) war für alle reellen λ_t mit $\lambda_1 = 1$ erfüllt, und da sie nach oben unbeschränkt ist, besitzt sie kein Maximum.

Es bleibt noch die Formel (1.36) zu beweisen. Aus (1.42), (1.44) und der Multiplikativität von g folgt

$$\frac{\lambda_t}{\gamma(t)} = \sum_{b\le z/t}\mu(b)\eta_{tb}(z) = \sum_{b\le z/t}\frac{\mu(b)\mu(tb)}{g(tb)G(z)} = \frac{\mu(t)}{g(t)}\cdot\frac{1}{G(z)}\sum_{\substack{b\le z/t\\ \mathrm{ggT}(b,t)=1}}\frac{\mu^2(b)}{g(b)}$$

denn für alle Paare b, t mit $\mathrm{ggT}(b,t) > 1$ ist die Zahl bt quadratvoll und deshalb ist $\mu(bt) = 0$. Wegen (1.38) und der Definition von $G_t(z/t)$ folgt daraus die Formel (1.36).

□

1.7 Anwendung auf das PZd-Problem

Aus der eben vorgestellten Siebmethode von Selberg folgen eine ganze Reihe von Anwendungen. Ein Beispiel dafür ist ein ganz allgemeines Ergebnis, aus dem sich vielfältige siebtheoretische Aussagen herleiten lassen. Der Beweis dieses Satzes ist nicht schwer jedoch umfangreich, und deshalb wird hier auf ihn verzichtet. Der Leser sei z.B. auf das Buch von Prachar [31] S. 45ff verwiesen.

Satz 1.7.1 *(Prime k-Tupel) Seien für $i = 1, \ldots, k$ die ganzzahligen Polynome $h_i(n) = a_i n + b_i$ gegeben derart, daß*

$$a_i \neq 0 \ \wedge \ \mathrm{ggT}(a_i, b_i) = 1 \qquad i = 1, \ldots, k$$

und daß

$$D := \prod_{i \leq k} a_i \prod_{j \leq k,\ j \neq i} (a_i b_j - a_j b_i) \neq 0$$

ist.

Sei $h(n) = \prod_i h_i(n)$, und $\beta(p)$ sei die Anzahl der inkongruenten Lösungen der Kongruenz $h(n) \equiv 0 \bmod p$.
Nehmen wir an, daß $\beta(p) < p$ für alle p ist. Dann gilt für alle $N \geq 2$:

$$\begin{aligned} & \#\{n \leq N : h_i(n) \text{ sind alle gleichzeitig prim für } i = 1, \ldots, k\} \\ < \ & C(k) \frac{N}{\log^k N} \prod_{p \mid D} \left(1 - \frac{1}{p}\right)^{-(k - \beta(p))} . \end{aligned} \tag{1.45}$$

Dabei hängt die positive Konstante $C(k)$ nur von k, nicht aber von N und der Wahl der h_i ab.

Beweis: Vgl. Prachar [31] S.45 ff. Den Beweis für ein etwas genaueres Ergebnis findet man auch in Halberstam, Richert [19] S.172 ff.

□

Mit diesem Satz wollen wir unser mit der Brunschen Methode erzieltes Ergebnis des Satzes 1.5.2 verbessern.

Satz 1.7.2 *Sei $d \geq 2$ gerade. Dann gilt*

$$\pi_d(N) < \frac{c(2)d}{\phi(d)} \frac{N}{\log^2 N}. \tag{1.46}$$

Beweis: Setzt man im Satz 1.7.1 $k = 2$, $a_1, b_1, a_2, b_2 = 1, 0, 1, d$, dann erhalten wir das Polynom $h(n) = n(n + d)$, und es ist $D = d \neq 0$. Wie wir in (1.9) gesehen haben, gilt $\beta(p) < p$ für alle p. Mit dem Satz 1.7.1 folgt dann die Ungleichung (1.45) für $\pi_d(N + d)$ und mit einer abgeänderten Konstanten die Behauptung.

□

Bemerkung 1: Bei $\phi(d)$ handelt es sich um die sog. **Eulersche** ϕ-Funktion, die für alle natürlichen Zahlen folgendermaßen definiert ist:

$$\phi = \mu * d = d \prod_{p|d} \left(1 - \frac{1}{p}\right) \tag{1.47}$$

und die Anzahl der zu n teilerfremden natürlichen Zahlen $\leq n$ angibt.
Bemerkung 2: Läßt man auch negative Primzahlen zu, so daß $p < N$ eine positive Primzahl und $p - d$ eine negative Primzahl ist, dann läßt sich mit dem Polynom $n(n - d)$ analog auch die obere Schranke für die Anzahl der Primzahlen $p \leq N$ angeben, für die eine negative Primzahl $p - d$ existiert, so daß die gerade Zahl d eine Zerlegung als Summe zweier Primzahlen hat. Es gilt

$$\#\{p \leq N, d = p + |p - d|\} < \frac{c(2)d}{\phi(d)} \frac{N}{\log^2 N},$$

womit wir eine obere Schranke für das Goldbachsche Problem gewinnen. Diese Ungleichung verliert natürlich ihren Sinn, falls $N > d$ wird. Deshalb können wir dieses Ergebnis etwas genauer formulieren im

Satz 1.7.3 *Sei $N \geq 2$ eine gerade Zahl. Dann ist die Anzahl der Darstellungen von N als Summe zweier Primzahlen beschränkt durch*

$$\#\{p \leq N, N = p + p'\} < \frac{c(2)N}{\phi(N)} \frac{N}{\log^2 N}. \tag{1.48}$$

□

1.8 Bericht über untere Schranken

Bis heute gibt es keine Siebmethode für untere Schranken, die an Einfachheit an die Selbergesche Methode für obere Schranken heranreichen würde.

In diesem Abschnitt sollen die wesentlichen Ideen und Ergebnisse vorgestellt werden, die im Laufe der Zeit zu diesem Thema entstanden sind. Eine relativ umfassende Darstellung der Siebmethoden für untere Schranken befindet sich in Halberstam, Richert [19], wonach sich deshalb der folgende Text vorwiegend richtet. Da es dem Verfasser lediglich darum geht, die Ideen für Konstruktionen unterer Schranken vorzustellen, wird hier, nicht zuletzt aus Platzgründen, gänzlich auf Beweise der Lemmata und Sätze verzichtet. Der Leser kann sie ohne Ausnahme in den Kapiteln 7 - 11 des Buches von Halberstam und Richert nachschauen.

Wie vorhin sei $\mathcal{P}$ eine unendliche Teilmenge aller Primzahlen, etwa die Menge $\mathcal{P} = \mathcal{P}_d := \{p\ prim, p \nmid d\}$. Ferner setzen wir für $z \geq 2$

$$P(z) := \prod_{p \in \mathcal{P},\ p<z} p.$$

Anders als in vorigen Abschnitten wird hier also die obere Grenze z nicht zugelassen, was insbesondere dann entscheidend ist, wenn z selbst eine Primzahl ist. Diese Definition wird hier aus Halberstam und Richert übernommen, weil manche Ergebnisse, die hier zitiert werden, gerade für prime z formuliert werden.

Für die endliche Menge verschiedener natürlicher Zahlen $\mathcal{A} = \{a_1, \ldots, a_N\}$ bezeichne A_t die Teilmenge von $\mathcal{A}$, deren Elemente durch t teilbar sind. Die Menge $\mathcal{A}$ soll wieder so beschaffen sein, daß es eine multiplikative Funktion β gibt, die für alle $p \in \mathcal{P}$ die folgende Bedingung erfüllt:

$\beta(p) := \#$ inkongruenter Restklassen mod p, in die alle $a \in \mathcal{A}$ fallen.

Für quadratfreie t lassen sich damit die Mächtigkeiten der A_t mit dem Bruch $\frac{\beta(t)}{t}N$ approximieren mit den "Fehlertermen"

$$R_t := \#\mathcal{A}_t - \frac{\beta(t)}{t}N.$$

Wir definieren ferner die Siebe

$$S(\mathcal{A}, \mathcal{P}, z) := \#\{a \in \mathcal{A} : \mathrm{ggT}(a, P(z)) = 1\}$$

und für quadratfreie t mit $\mathrm{ggT}(t, \mathcal{P}_1 \backslash \mathcal{P}) = 1$, also alle, die außerdem zu allen Primzahlen $p|d$ *teilerfremd* sind

$$S(\mathcal{A}_t, \mathcal{P}, z) := \#\{a \in \mathcal{A}_t : \mathrm{ggT}(a, P(z)) = 1\}.$$

Dabei ist offensichtlich, daß das letzte Sieb nichttrivial nur für $\mathrm{ggT}(t, P(z)) = 1$ wird, da ansonsten die $a \in \mathcal{A}_t$ vollständig durch Primzahlen $p|t$, $p \in \mathcal{P}$, $p < z$ ausgesiebt würden. Schließlich definieren wir noch das Produkt

$$W(z) := \prod_{p \in \mathcal{P},\ p<z} \left(1 - \frac{\beta(p)}{p}\right).$$

Eine erste untere Schranke kann aus der folgenden Identität[39] gewonnen werden:

Lemma 1.8.1 *Für $2 \leq z_1 \leq z$ gilt*

$$S(\mathcal{A}_t, \mathcal{P}, z) = S(\mathcal{A}_t, \mathcal{P}, z_1) - \sum_{z_1 \leq p < z} S(\mathcal{A}_{tp}, \mathcal{P}, p) \tag{1.49}$$

und

$$W(z) = W(z_1) - \sum_{z_1 \leq p < z} \frac{\beta(p)}{p} W(p). \tag{1.50}$$

Hat man nun für $S(\mathcal{A}_t, \mathcal{P}, z_1)$ entweder eine untere Schranke oder eine asymptotische Formel, z.B. wenn z_1 klein genug gegenüber N ist, und schätzt man die Terme $S(\mathcal{A}_{tp}, \mathcal{P}, p)$ nach oben ab, dann liefert (1.49) eine nichttriviale untere Schranke, vorausgesetzt sie ist positiv.

Zunächst einmal wird also eine asymptotische Formel für die $S(\mathcal{A}_t, \mathcal{P}, z_1)$ benötigt. Eine solche Formel kann gewonnen werden, wenn an die multiplikative Funktion β zwei Bedingungen gestellt werden.

Bedingung 1.8.1 *Für alle Primzahlen $p \in \mathcal{P}$ kann $\beta(p)$ nicht beliebig nahe an p kommen, genauer existiert eine Konstante $K_1 > 1$ mit*

$$0 \leq \frac{\beta(p)}{p} \leq 1 - \frac{1}{K_1} \qquad \forall p \in \mathcal{P}.$$

Bedingung 1.8.2 *Es gibt eine positive konstante "Siebdimension" k, die angibt, wie groß (zumindest im Durchschnitt) $\beta(p)$ für alle $p \in \mathcal{P}$ werden kann, genauer soll es eine Konstante $K_2 \geq 1$ geben mit*

$$\sum_{y_1 \leq p < y_2} \frac{\beta(p)}{p} \log p = k \log \frac{y_2}{y_1} + K_2.$$

[39] Der erste, der diese Identität erfolgreich in der Siebtheorie eingesetzt hat, war Buchstab [8].

Satz 1.8.1 *Unter den Bedingungen 1.8.1 und 1.8.2 gilt für $\xi \geq z_1$ eine für $N \to \infty$ asymptotische Formel*

$$\begin{aligned} S(\mathcal{A}_t, \mathcal{P}, z_1) &= \frac{\beta(p)}{p} W(z_1) N \left\{ 1 + \mathcal{O}\left(\frac{1}{(\tau+1)^\tau} \right) \right\} \\ &\quad + \theta \sum_{s|P(z_1),\ s<\xi^2} 3^{\omega(s)} |R_{ts}| \end{aligned} \tag{1.51}$$

mit $\tau = \frac{\log \xi}{\log z_1}$, $|\theta| \leq 1$.

Der Beweis besteht darin, daß man aus anderen analytischen Ergebnissen der Siebtheorie (vgl. etwa Halberstam, Richert Satz 6.2) für $S(\mathcal{A}_t, \mathcal{P}, z_1)$ eine obere Schranke und aus der Identität des Lemmas 1.8.1 eine untere Schranke gewinnt und zeigt, daß diese Schranken dieselbe asymtotische Größenordnung haben. Der Ausdruck $3^{\omega(s)}$ im Fehlerterm stammt von der Anzahl der Möglichkeiten, daß zwei Teiler $s_1, s_2 | P(z_1)$ ein quadratfreies gemeinsames Vielfaches bilden.

Der Satz 1.8.1 liefert nur nichttriviale Ergebnisse, falls N sehr viel größer als z_1 ist, also wenn $u := \log N / \log z_1$ groß ist. Um ein Ergebnis für endliche u zu erhalten, das sich dann als untere Schranke für $S(\mathcal{A}_t, \mathcal{P}, z)$ und schließlich mit einer Zusatzvoraussetzung für $S(\mathcal{A}, \mathcal{P}, z)$ benutzen läßt, studiert man die Eigenschaften gewisser Differenzen-Differentialgleichungen. Ist $\gamma = 0,577215665\ldots$ die Eulersche Konstante, dann lassen sich mit

$$\begin{aligned} \sigma_k(u) &:= \frac{u^k}{(2e^\gamma)^k \Gamma(k+1)}, \qquad 0 \leq u \leq 2 \\ \left(\frac{\sigma_k(u)}{u^k} \right)' &= \frac{-k\sigma_k(u-2)}{u^{k+1}}, \qquad u > 2 \end{aligned}$$

für $u > 1$ die folgenden Funktionen definieren[40]

$$\eta_k(u) = \frac{k}{u^k} \int_u^\infty \frac{1}{t^{k-1}} \left(\frac{1}{\sigma_k(t-1)} - 1 \right) dt, \qquad u > 1. \tag{1.52}$$

Diese Funktionen haben viele interessante Eigenschaften (vgl. Halberstam, Richert S. 193-197, S. 211-213). Man weiß beispielsweise, daß $\eta_k(u)$ nicht negativ für $u > 1$ und dort streng monoton fallend ist. Weiter weiß man, daß die Gleichung

$$\eta_k(u) - 1 = 0$$

[40]Man verlangt noch die Stetigkeit von $\sigma_k(u)$ für $u = 2$.

für ein $u = u_k$ eine für jedes k eindeutig definierte Nullstelle besitzt, die man für kleine k numerisch bestimmen kann[41]. Wie sich gleich herausstellen wird, spielen die Nullstellen von η_k eine entscheidende Rolle, da in der folgenden unteren Abschätzung der Korrekturfaktor $-\eta_k(2\tau)$ mit $\tau = \log\xi/\log z$ auftaucht. Liegt nun 2τ nahe bei u_k, dann vernichtet dieser (negative) Korrekturfaktor den Hauptterm, und unsere Schranke wird trivial.
Wir schwächen nun die Bedinung 1.8.2 etwas ab in der

Bedingung 1.8.3 *Es gibt zwei Konstanten $K_2, K_3 \geq 1$ mit*

$$-K_3 \leq \sum_{y_1 \leq p < y_2} \frac{\beta(p)}{p} \log p - k \log \frac{y_2}{y_1} \leq K_2.$$

Das Ergebnis für untere Schranken lautet nun folgendermaßen:

Satz 1.8.2 *Unter den Bedingungen 1.8.1 und 1.8.3 gilt für $\xi \geq z$ und $N \to \infty$ die untere Abschätzung*

$$\begin{aligned} S(\mathcal{A}_t, \mathcal{P}, z) \geq\ & \frac{\beta(p)}{p} W(z) N \left\{ 1 - \eta_k(2\tau) + \mathcal{O}\left(\frac{K_3 (\log\log 3\xi)^{3k+2}}{\log \xi} \right) \right\} \\ & - \sum_{s | P(z),\ s < \xi^2} 3^{\omega(s)} |R_{ts}| \end{aligned} \tag{1.53}$$

mit $\tau = \frac{\log\xi}{\log z}$.

Man sieht also, daß man $2\tau > u_k$ wählen muß, damit dieser Satz nichttrivial wird. Dies wiederum vergrößert ξ, wodurch die Anzahl der Terme in (1.53) möglicherweise zu groß wird. Um ein allgemeines Ergebnis zu bekommen, brauchen wir also eine weitere Zusatzbedingung:

Bedingung 1.8.4 *Es gibt von k abhängige Konstanten α, $0 < \alpha < 1$, $K_4 \geq 1$, $K_5 \geq 1$, so daß für alle $N \geq 2$ gilt*

$$\sum_{\substack{s < N^\alpha / (\log N)^{K_4} \\ \mathrm{ggT}(s, \mathcal{P} \setminus \mathcal{P}_d) = 1}} \mu^2(s) 3^{\omega(s)} |R_s| \leq K_5 \frac{N}{\log^{k+1} N}.$$

[41] vgl. Ankeny, Onishi [2], Porter [30] oder deren Zitate in Halberstam, Richert.

Damit läßt sich aus Satz 1.8.2 für $t = 1$ die folgende untere Schranke gewinnen:

Satz 1.8.3 *Unter den Bedingungen 1.8.1, 1.8.3 und 1.8.4 gilt für*

$$z^2 \le \frac{N^\alpha}{(\log N)^{K_4}}$$

und für $N \to \infty$ die untere Abschätzung

$$S(\mathcal{A}, \mathcal{P}, z) \ge W(z)N \left\{1 - \eta_k \left(\alpha \frac{\log N}{\log z}\right) + \mathcal{O}\left(\frac{K_3 (\log\log 3N)^{3k+2}}{\log N}\right)\right\}.$$

Wir können diesen Satz auf Primzahlzwillinge anwenden. Wählt man $\mathcal{A} = \{p + d; p \le x\}$ und $\mathcal{P} = P_d$ für gerade $d \ge 2$, dann ist die Bedingung 1.8.1 erfüllt (vgl. Abschnitt 1.4). Man kann zeigen (vgl. Halberstam, Richert, Ergebnisse (5.1.1) und (3.7.4)), daß für $k = 1$ und $\alpha = 1/2$ auch die beiden anderen Voraussetzungen des Satzes erfüllt sind. Wählt man nun

$$z^2 = N^{1/u}$$

mit einem $u = 2.1$ (dies ist eine Zahl, die etwas größer ist, als die für $k = 1$ numerisch ermittelte[42] Nullstelle $u_1 = 2.06\dots$), dann folgt aus dem Satz 1.8.3, daß es eine von d abhängige Konstante $\delta > 0$ und ein $N_0 \in \mathbb{N}$ gibt, so daß für alle $n > N_0$

$$\#\{p \le n : \mathrm{ggT}(p + d, P(z)) = 1\} \ge \delta \frac{n}{\log^2 n}$$

ist. Die verbleibenden Zahlen $p + d < n + d$ haben also die Eigenschaft, daß alle ihre Primfaktoren q die Bedingung

$$N^{\Omega(p+d)/4.2} = z^{\Omega(p+d)} \le q^{\Omega(p+d)}$$

erfüllen, wenn $\Omega(p+d)$ die Anzahl aller (nicht unbedingt verschiedener) Primfaktoren von $p + d$ bezeichnet. Daraus folgt insbesondere, daß es für jedes gerade $d \ge 2$ unendlich viele Primzahlen p gibt, so daß $p + d$ höchstens ein P_4 ist[43].

Durch iterierte Anwendung der Identität des Lemmas 1.8.1 lassen sich für $k = 1$ unter großem Rechenaufwand einige im Vergleich zum Satz 1.8.3 bessere Ergebnisse[44] erzielen, die jedoch in Bezug auf Anwendungen qualitativ

[42] vgl. Ankeny, Onishi [2]

[43] Zur Erinnerung bezeichnen wir mit P_r jede ganze Zahl m mit $\Omega(m) \le r$.

[44] vgl. Halberstam, Richert Kap.8

keine schärferen Resultate erlauben. Für $k > 1$ ist es nie gemacht worden, da man für die Iteration sehr komplizierte Ausdrücke für die (dann neuen) Funktionen η_k braucht.

Kuhn [27] schlug 1941 als erster vor, man könne eine mächtigere Siebmethode für untere Schranken konstruieren, falls man die Summen

$$\sum_{\substack{a\in\mathcal{A}\\ \mathrm{ggT}(a,P(z))=1}} \left(1-\sum_{p|a} w_p\right) \qquad \text{statt} \qquad \sum_{\substack{a\in\mathcal{A}\\ \mathrm{ggT}(a,P(z))=1}} 1$$

betrachtet, mit noch zu wählenden Gewichten w_p für alle $p \in \mathcal{P}$. In der Tat sind die besten Ergebnisse, die mittels einer Siebmethode für untere Schranken bis jetzt bewiesen worden sind, eine Kombination des Selbergschen Siebes mit Kuhnschen Gewichten. Im Laufe der Zeit sind verschiedene Gewichtsfunktionen ausprobiert worden. In Verbindung mit der Brunschen Methode (für untere Schranken) studierte 1947 Rényi [33] die gewichtete Summe

$$\sum_{\substack{p<2N\\ \mathrm{ggT}(2N-p,P(z))=1}} \log p \exp\left(-p\frac{\log 2N}{2N}\right)$$

und kam zu dem Schluß, daß für genügend große N immer eine Gleichung $2N = p + P_r$ gefunden werden kann, wobei r beschränkt bleibt. Buchstab [9] formulierte die Suche nach geeigneten Gewichten als ein Problem der linearen Programmierung und kam zu einer sehr komplizierten Menge von konstanten Gewichten. Mit seiner Methode (vgl. auch Buchstab [10]) konnte er sogar $2N = p + P_3$ zeigen. Halberstam und Richert waren der Meinung, daß jedes Siebproblem möglicherweise seine eigene Optimierung der Gewichte erfordert, um die bestmöglichen Ergebnisse zu erzielen. Trotzdem konnten sie das Ergebnis von Buchstab auch mit einfacheren, von Ankeny und Onishi erfundenen und von Richert weiterentwickelten Gewichten erzielen. Sie definierten die Gewichte mit einem für das jeweilige Siebproblem geeigneten Parameter λ wie folgt:

$$w_p := \begin{cases} \lambda\left(1-\frac{u\log p}{\log N}\right), & \text{falls } N^{1/v} \le p < N^{1/u} \\ 0 & \text{sonst,} \end{cases}$$

für alle $p \in \mathcal{P}$ und eine feste Wahl von $u < v$. Auf diese Weise gewinnt man eine Möglichkeit, siebende Primzahlen gewisser Größenordnung besonders hervorzuheben. Die Idee besteht nun darin, die gewichtete Summe

$$W(\mathcal{A},\mathcal{P},v,u,\lambda) :=$$

$$\sum_{\substack{a\in\mathcal{A} \\ \mathrm{ggT}(a,P(N^{1/v}))=1}} \left(1-\lambda \sum_{\substack{p|a,p\in\mathcal{P} \\ N^{1/v}\le p<N^{1/u}}} \left(1-\frac{u\log p}{\log N}\right)\right) \tag{1.54}$$

nach unten abzuschätzen. Die Wahl von λ, u und v muß so geschehen, daß die rechte Seite positiv wird. Dies impliziert dann, daß $\mathcal{A}$ Elemente enthält, für die

$$\lambda^{-1} > \sum_{\substack{p|a,p\in\mathcal{P} \\ N^{1/v}\le p<N^{1/u}}} \left(1-\frac{u\log p}{\log N}\right)$$

gilt. Dies wiederum, daß jedes solche a nur relativ wenige Primfaktoren haben kann: Sie müssen größer als $N^{1/v}$ sein und kleiner als $N^{1/u}$. Ist $1/u$ nahe bei $1/2$, können solche a nur noch sehr wenige, große Primfaktoren besitzen.

Zur Abschätzung von (1.54) nach unten verfährt man ähnlich wie vorhin. Als erstes definiert man geeignete Differenzen-Differentialgleichungen:

$$w(u) = \frac{1}{u}, \quad \rho(u) = 1, \qquad \text{für } 0 < u \le 2$$

$$(uw(u))' = w(u-1), \quad (u-1)\rho'(u) = -\rho(u-1), \qquad \text{für } u \ge 2$$

und mit ihnen die Funktionen

$$F(u) := e^{\gamma}\left(w(u) + \frac{\rho(u)}{u}\right), \qquad u > 0 \tag{1.55}$$

und

$$f(u) := e^{\gamma}\left(w(u) - \frac{\rho(u)}{u}\right), \qquad u > 0. \tag{1.56}$$

Neben vielen anderen Eigenschaften von $F(u)$ und $f(u)$ kann man zeigen (vgl. Halberstam&Richert), daß

$F(u)$ monoton fallend ist und $\lim_{u\to\infty} F(u) = 1+$

$f(u)$ monoton wachsend ist und $\lim_{u\to\infty} f(u) = 1-$

Bemerkung: In Brüdern [5] Kap. 5.4 findet man eine andere interessante Differenzen-Differentialgleichung $\rho_0(u)$. Dort wird gezeigt:
Es gibt genau eine stetige Funktion, $\rho_0 :]0, \infty[\to \mathbb{R}$, die auf $]1, \infty[$ differenzierbar ist und den Bedingungen

$$\rho_0(u) = 1, \textit{ für } 0 < u \leq 1, \quad u\rho_0'(u) = -\rho_0(u-1), \qquad \textit{für } u > 1$$

genügt. Es gilt $0 < \rho_0(u) < 1$ für $u > 1$, dort ist ρ_0 auch streng monoton fallend. Überdies gilt für jedes gegebene ϵ mit $0 < \epsilon < 1$ und für $n \geq 2$, $y \geq n^\epsilon$ die asymptotische Formel

$$\begin{aligned} \Psi(n, y) &:= \#\{m = 1, \ldots, n : \text{gPf}(m) \leq y\} \\ &= n\rho_0\left(\frac{\log n}{\log y}\right) + \mathcal{O}\left(\frac{n}{\log n}\right). \end{aligned} \tag{1.57}$$

Dabei bezeichnet $\text{gPf}(m)$ den größten Primfaktor von m. Die Funktion $\Psi(n, y)$ ist in letzter Zeit Gegenstand intensiver Forschung (vgl. etwa Fouvry, Tanenbaum [17]).

Halberstam und Richert bewiesen das folgende Ergebnis

Satz 1.8.4 *Seien die Bedingungen 1.8.1, 1.8.3 und 1.8.4 mit $k = 1$ erfüllt. Ferner gebe es von N unabhängige Zahlen u, v und K_6, die*

$$1/\alpha < u < v$$

und

$$0 < \lambda \leq K_6$$

erfüllen. Dann gilt

$$\begin{aligned} &W(\mathcal{A}, \mathcal{P}, v, u, \lambda) \geq W(N^{1/v})N \\ &\times \left\{ f(\alpha v) - \lambda \int_u^v F\left(v\left(\alpha - \frac{1}{t}\right)\right)\left(1 - \frac{u}{t}\right)\frac{dt}{t} - C\frac{K_3}{(\log N)^{1/14}} \right\}, \end{aligned}$$

wobei die Konstante C nur von u, v, α und den K_i abhängt.

Der Beweis dieses Satzes ist sehr kompliziert und erfordert diverse Ergebnisse, die man aus der Iteration der Identität aus dem Lemma 1.8.1 erzielen kann. In bezug auf seine Anwendung ist der Satz jedoch nicht befriedigend, da man f und F nur für kleine Werte des Arguments kennt. Halberstam und Richert zeigten jedoch nach einer relativ kurzen Rechnung, daß man den Ausdruck in geschweiften Klammern des Satzes 1.8.4 unter Umständen durch einfachere Funktionen ersetzen kann:

Lemma 1.8.2 *Für*

$$\frac{1}{\alpha} < u < v, \qquad \frac{2}{\alpha} \le v \le \frac{4}{\alpha}, \qquad \lambda \ge 0$$

gilt

$$f(\alpha v) - \lambda \int_u^v F\left(v\left(\alpha - \frac{1}{t}\right)\right)\left(1 - \frac{u}{t}\right)\frac{dt}{t}$$

$$= \frac{2e^\gamma}{\alpha v}\left\{\log(\alpha v - 1) - \lambda \alpha u \log\frac{v}{u} + \lambda(\alpha u - 1)\log\frac{\alpha v - 1}{\alpha u - 1}\right\}.$$

Mit dieser Vereinfachung des Satzes 1.8.4 wendeten Halberstam und Richert diesen Satz auf das PZd-Problem und das Goldbachsche Problem an. Sie wählten für ein gerades $d \ge 2$ die Folge $\mathcal{A} = \{p + d : p \le M\}$, $N = li\ M$, $\mathcal{P} = \mathcal{P}_d$ und $\beta(p) = p/(p-1)$ für alle $p \in \mathcal{P}$. Mit den Ergebnissen (3.6.8) und (3.7.4) ihres Buches zeigten sie, daß die Bedingung 1.8.4 für $k = 1$ und $\alpha = 1/2$ erfüllt ist. Die Bedingungen 1.8.1 und 1.8.3 zeigten sie mit den Ergebnissen (5.1.1) und (5.1.5). Der Satz 1.8.4 ist somit anwendbar. Nach geschickter Wahl der Parameter u,v und λ[45] und der mit dem Ergebnis 5.2.5 ihres Buches erfolgten Auswertung des Produkts $W(N^{1/v})$ bewiesen sie den folgenden

Satz 1.8.5 *Es gibt eine positive Zahl M_0, so daß für alle $M \ge M_0$ und jede gerade Zahl d mit $0 < |d| \le M$ gilt*

$$\#\{p \le M : p + d = P_3\} \ge \frac{13}{3} C_2 \prod_{2<p|d} \frac{p-1}{p-2} \frac{M}{\log^2 M}$$

mit der auf Seite 5 definierten Konstanten C_2. Falls M gerade ist, so ist

$$\#\{p \le M : M - p = P_3\} \ge \frac{13}{3} C_2 \prod_{2<p|d} \frac{p-1}{p-2} \frac{M}{\log^2 M}.$$

[45] Gewählt wurde $u = \frac{8}{3}$, $v = 8$ und $\lambda > \frac{3}{4}$.

Überraschenderweise unterscheidet sich dieses Ergebnis nur in der Konstanten 13/3 von der für d-Zwillinge formulierten Hardy-Littlewoodschen Vermutung (1.1) mit der Konstanten 2. Als Bemerkung zum Beweis des Satzes sei noch angeführt, daß das Ergebnis für $M - p = P_3$ aus dem Ergebnis für $p + d = P_3$ folgt, wenn man $d = -M$ wählt. Denn wir haben die Fastprimzahlen P_r als nicht unbedingt positive Zahlen definiert.

Halberstam und Richert merkten an, daß man auf eine ähnliche Art ein Ergebnis für $M - p = P_2$ erzielen könnte, wäre im Satz 1.8.4 die Wahl von $1/2 < \alpha = 0.546$ erlaubt. Dies scheitert jedoch an der Abschätzung der Restglieder aus der Bedingung 1.8.4, für die aus gewissen Gründen (Satz von Bombieri)

$$\sum_{s<N^\alpha/(\log N)^{K_4}} \mu^2(s)3^{\omega(s)}|R_s| = \mathcal{O}\left(\frac{N}{\log^3 N}\right)$$

nur mit einem K_4 wählbar ist, falls man $\alpha = 1/2$ voraussetzt. Halberstam und Richert vermuteten auch, daß man mit einem weiteren Trick, nämlich dem nachträglichen Aussieben von Repräsentierungen der Form $M - p = P_3$, eine untere Schranke für $M - p = P_2$ finden kann. Genau dies ist unabhängig von diesen Feststellungen Jing-run Chen in [13] gelungen. Er zeigte den

Satz 1.8.6 *Es gibt eine positive Zahl M_0, so daß für alle $M \geq M_0$ und jede gerade Zahl d mit $0 < |d| \leq M$ gilt*

$$\#\{p \leq M : p + d = P_2\} \geq 0.67 \cdot C_2 \prod_{2<p|d} \frac{p-1}{p-2} \frac{M}{\log^2 M}$$

mit der auf Seite 5 definierten Konstanten C_2. Falls M gerade ist, so ist

$$\#\{p \leq M : M - p = P_2\} \geq 0.67 \cdot C_2 \prod_{2<p|d} \frac{p-1}{p-2} \frac{M}{\log^2 M}.$$

Den relativ komplizierten Beweis dieses bis heute besten Ergebnisses dieser Art findet der Leser in der Originalarbeit von Chen oder im 11. Kapitel des Buches von Halberstam und Richert.

Kapitel 2

Über die Frage, wann die Zahlen $6n - 1, 6n + 1$ gleichzeitig zusammengesetzt sind.

Der Titel dieses Kapitels mag vielleicht überraschen. Denn die Beantwortung der Titelfrage scheint auf den ersten Blick nur wenig mit dem Primzahlzwillingsproblem gemeinsam zu haben. Genauer genommen wird uns hier das PZ2-Problem interessieren. In diesem Kapitel werden wir zeigen, daß man eine Antwort auf die Titelfrage sehr wohl als Lösungsansatz des PZ2-Problems heranziehen kann. Von der Qualität dieser Antwort, eben wie gut wir die Anzahl solcher simultan zusammengesetzter Zahlen $6n - 1, 6n + 1$, sagen wir mal bis $n \leq N$ (nach unten) abschätzen können, wird dann abhängen, ob und wie gut wir eine untere Schranke für 2-Zwillinge konstruieren können. Der Zusammenhang mit dem PZ2-Problem wird insbesondere im Abschnitt 2.3 deutlich. Danach werden wir zuerst die kombinatorischen Gesetze studieren, die dem Zustandekommen simultan zusammengesetzter Zahlen $6n-1, 6n+1$ zugrundeliegen. Dies wird uns eine genaue, da kombinatorisch begründete, Formel für die Anzahl solcher Paare für bestimmte N liefern. Die Natur des PZ2-Problems erfordert jedoch eine asymptotische Formel für beliebige n. Im Abschnitt 2.6 wird sich herausstellen, daß das Problem, eine untere Schranke für 2-Zwillinge aufzustellen, zumindest formelmäßig faßbar ist mit einem Hauptterm der Größenordnung $cN/\log^2 N$ und mit einem Fehlerterm der Größenordnung $o\left(N/\log^2 N\right)$. Leider wird uns der Übergang von unserer genauen kombinatorischen Formel für bestimmte N auf beliebige n einen zweiten unbekannten Fehlerterm bescheren. Bei diesem Übergang werden wir annehmen, daß die Zählfunktion solcher zusammengesetzter Paare $6\nu - 1, 6\nu + 1$ für $\nu = 1, \ldots, n$ einigermaßen "vernünftig" wächst und keine allzugroßen Sprungstellen aufweist. In anderen Worten werden wir für dieses kleine n einen "Mittelwert" als Zählfunktion heranziehen, der aus der bekannten Formel für große N mit dem Wichtungsfaktor n/N entsteht. Ob sich die dabei entstehende (wohl bemerkt in dieser Arbeit nicht bestimmte) Abweichung zur wirklichen Anzahl solcher Paare jemals wird abschätzen lassen, sei dahingestellt.

Doch in den ersten zwei Abschnitten möchte der Verfasser Überlegungen darlegen, die sich ihm während der Arbeit am PZd-Problem automatisch als Nebenprodukt aufgedrängt haben. Obwohl sie ein wenig aus dem Rahmen dieses Kapitels fallen, behandeln sie interessante Fragestellungen, die nach Meinung des Verfassers bis heute in der Literatur zu kurz gekommen sind. Auf jeden Fall eignen sie sich gut als Einführung für die darauffolgenden Abschnitte.

2.1 Das PZ2-Problem und zugehörige Siebkonstruktionen

In der Literatur, wie auch in dieser Arbeit in den Abschnitten 1.1.4 bis 1.1.8, wird das PZd-Problem meist so behandelt, daß die Folge $\mathcal{A}$ als die Wertemenge des Polynoms $a_\nu = \nu(\nu + d)$ gewählt wird[1]. Legt man die Siebdefinition 1.1.3.1 zugrunde, läuft es aufs gleiche hinaus, wenn man $\mathcal{A} = \{1, \ldots, N\}$ setzt und als siebende Restklassen 0 und $-d$ modulo aller Primzahlen $p \nmid d$ und 0 modulo aller Primzahlen $p|d$ wählt[2]. Für Ungeübte entsteht so der irrtümliche Eindruck, daß das Polynom $\nu(\nu + d)$ das einzige sei, mit dem man das PZd-Problem modellieren könne.

Wir werden gleich sehen, daß dies nicht die einzige mögliche Wahl ist. Obwohl die Wahl eines anderen Polynoms keine qualitative Verbesserung für siebtheoretische Ergebnisse mit sich bringt[3], kann dies numerische Vorteile bewirken - man findet mehr Primzahlzwillinge mit weniger Rechenaufwand. Außerdem wird die gesiebte Untermenge der natürlichen Zahlen unter

[1] vgl. für $d = 2$ Halberstam&Richert [19] S. 27ff, Schwarz [35] (S. 41ff), Prachar [31] (S. 33ff)

[2] vgl. Brüdern [5] (S. 179ff), Landau [28] (S. 73ff)

[3] bezogen auf PZd-Probleme also primär Ergebnisse über obere Schranken

Umständen transparenter. Um es zu demonstrieren, zeigen wir es am Beispiel der 2-Zwillinge. Für eine feste Anzahl $n = 100$ der Polynomwerte $h(\nu)$ geben wir nun die Größen $h(\nu)$ und $\mathcal{P}$ an. Alles Weitere folgt dann aus der Definition 1.1.3.2. Es lassen sich folgende verschiedener **Zwillingssiebe** für $d = 2$ konstruieren:

1. $h(\nu) = \nu(\nu+2)$ für ungerade ν mit $\mathcal{P} = \{2 < p \leq \sqrt{n}\}$ (herkömmliche Wahl). Das Ergebnis für $n = 100$:

   $$S = \#\{11, 17, 29, 41, 59, 71\}.$$

   Es bleiben also alle Primzahlen p im Intervall $]10, 100]$ übrig, für die auch $p + 2$ Primzahl ist. Effizienz: 6 gefundene Zwillinge[4].

2. $h(\nu) = 9\nu(\nu + 2) + 8$, ν ungerade
   $n = 100$
   $\mathcal{P} = \{2 < p \leq \sqrt{3n + 4}\}$
   Ergebnis:

   $$S = \#\{5, 9, 13, 19, 23, 33, 35, 45, 49, 59, 63, 65, 75, 79, 89, 93\},$$

   also alle Zahlen $\nu = 1, \ldots, 100$, für die die $3\nu+2$ und $3\nu+4$ Primzahlen sind und für die $3 \cdot 4 + 4 < 3\nu + 2 < 3\nu + 4 \leq 3 \cdot 100 + 4$ ist. Es wurden 16 Zwillinge gefunden.

3. $h(\nu) = 4\nu(\nu + 2) + 3$, $3 \nmid \nu$
   $n = 100$
   $\mathcal{P} = \{2 < p \leq \sqrt{2n + 4}\}$
   Ergebnis:

   $$S = \#\{8, 14, 20, 29, 35, 50, 53, 68, 74, 89, 95, 98\},$$

   also alle 12 Zahlen ν mit $2 \cdot 5 + 3 < 2\nu + 1 < 2\nu + 3 \leq 2 \cdot 100 + 3$, für die $2\nu + 1$ und $2\nu + 3$ Primzahlen sind.

---

[4]Nach Ansicht des Verfassers ist diese häufig in der o.g. Literatur anzutreffende Wahl auch deshalb unnötig kompliziert und didaktisch unglücklich gewählt, weil man mit der Wahl $2 \leq p \leq \sqrt{n}$ auf die Einschränkung ν ungerade verzichten könnte, wie im Abschnitt 1.1.4 geschehen ist. Sieht man dies das erste Mal, denkt man, diese Einschränkung sei irgendwie "wichtig".

4. $h(\nu) = (6\nu - 1)(6\nu + 1) = 36\nu^2 - 1$,
   $n = 100$
   $\mathcal{P} = \{3 < p \leq \sqrt{6n+1}\}$
   Ergebnis:

$$S = \#\{5, 7, 10, 12, 17, 18, 23, 25, 30, 32, 33, 38, 40, 45, 47, 52, 58, 70, 72, 77, 87, 95\},$$

   also alle Zahlen ν, für die das Paar $(6k-1, 6k+1)$ Primzahlzwillinge enthält. Hier ist die Effizienz 22. Dabei gilt wieder entsprechend $\sqrt{6 \cdot 100 + 1} < 6k - 1 < 6k + 1 \leq 6 \cdot 100 + 1$.

Die Siebkonstruktionen 2. und 4. haben den "Nachteil", daß sie die Zwillinge $(3, 5)$ nicht berücksichtigen, dafür aber liefern sie für ein festes n im Vergleich zu den Polynomen in 1. und 3. mehr Zwillinge. Die Konstruktion in 4. ist auch leichter zu formulieren als die drei anderen: Die Zusatzbedingungen an ν entfallen - es ist unerheblich, ob ν gerade, ungerade oder durch 3 teilbar ist. Es soll einfach nur eine natürliche Zahl sein.

Es bleibt natürlich zu zeigen, daß für jedes dieser Polynome nicht unvertretbar viele 2-Zwillinge ausgelassen werden[5]. Für $h(\nu) = \nu(\nu + 2)$ folgt dies sofort aus der Definition. Für die restlichen Polynome zeigen wir es am Beispiel des letzten Polynoms $h(\nu) = 36\nu^2 - 1$. Bezeichnen wir mit $\mathbb{N}_6$ die Menge aller zu 6 teilerfremden natürlichen Zahlen, dann finden wir, daß sie die Zahl 1 enthält und aus allen durch $6\nu-1$ oder $6\nu+1$ ($\nu \in \mathbb{N}$) darstellbaren Zahlen besteht und nur diesen, denn die Zahlen $6\nu \pm 2$ oder $6\nu \pm 3$ sind zu 6 nicht teilerfremd, doch genau aus diesem Grund sind sie auch durch 2 oder 3 teilbar. Deshalb können sie keine Primzahlen sein und folglich auch nie eine der Primzahlen in einem Primzahlzwilling $(p, p+2)$. Aus diesem Grund müssen alle Primzahlen $p > 3$ und somit auch alle 2-Zwillinge außer $(3, 5)$ in $\mathbb{N}_6$ liegen und die Form $(6\nu - 1)(6\nu + 1)$ haben[6].

Es wird nun klar, warum im vierten Beispiel die Primzahlen 2 und 3 ausgelassen und $\mathcal{P} = \mathbb{P}_6$ gesetzt wurde. Die Zahlen $6\nu - 1$ und $6\nu + 1$ sind nie durch 2 und 3 teilbar, und deshalb sind sie für die Siebkonstruktion unerheblich, würden aber auch nicht stören, hätte man sie zu $\mathcal{P}$ hinzugenommen.

[5] Bezugnehmend auf das PZ2-Problem ist es hier leider nicht möglich, "unendlich viele" zu sagen.

[6] Diese Feststellung ist sehr einfach und wurde schon mehrfach zitiert, vgl. z.B. Sheyser [37]

Wir finden nun, daß $\mathbb{N}_6$ teilergeschlossen ist, denn es gilt $\mathbb{N}_6 = \mathbb{P}_6^*$, wobei $\mathbb{P}_6^*$ die Menge aller aus den Primzahlen $p \nmid 6$ (also aller der Form $6\nu \pm 1$) darstellbaren Produkte vereinigt mit der Menge $\{1\}$ ist. Wir haben gesehen, das beim Polynom $\nu(\nu+d)$ die siebenden Restklassen 0 und $-d \bmod p$ waren. Wie sieht es aber im Fall $36\nu^2 - 1$ aus? Um diese Frage zu beantworten, betrachten wir zuerst die Tabelle 2.1.

$(6\nu-1, 6\nu+1)$	ν	5	7	11	13	17	19	23	25	$\cdots$
(5,7)	1	$\times$	$\times$							
(11,13)	2			$\times$	$\times$					
(17,19)	3					$\times$	$\times$			
23,25	4	$\times$						$\times$	$\times$	
(29,31)	5									
35,37	6	$\times$	$\times$							
(41,43)	7									
47,49	8		$\times$							
53,55	9	$\times$		$\times$						
(59,61)	10									
65,67	11	$\times$			$\times$					
(71,73)	12									
77,79	13		$\times$	$\times$						
83,85	14	$\times$				$\times$				
89,91	15		$\times$		$\times$					
95,97	16	$\times$					$\times$			
(101,103)	17									
(107,109)	18									
113,115	19	$\times$						$\times$		
119,121	20		$\times$	$\times$		$\times$				
125,127	21	$\times$							$\times$	
131,133	22		$\times$				$\times$			
(137,139)	23									
$\vdots$	$\vdots$									

Tabelle 2.1: Siebende Restklassen beim Polynom $h(\nu) = 36\nu^2 - 1$. Eingeklammert wurden Primzahlzwillinge.

Sie zeigt für jede der Zahlen $6\nu \pm 1$ (insbesondere also Primzahlen ¿3), wo die siebenden Restklassen angesiedelt sind. Um das Ergebnis zu formalisieren, definieren wir die Abbildung

$$\kappa : \mathbb{R} \to \mathbb{Z}, \qquad \kappa(a) := \left\lfloor \frac{a+1}{6} \right\rfloor \ \forall\, a \in \mathbb{R}.$$

Diese Abbildung ist nicht injektiv, aber surjektiv[7]. Genauer gilt

$$\kappa(1) = 0,\ \kappa(6\nu - 1) = \kappa(6\nu + 1) = \nu \text{ für alle } \nu \in \mathbb{N}.$$

Die Tabelle 2.1 zeigt, daß $\kappa(p)$ für jede Primzahl $p > 3$ gleichzeitig angibt, welche Restklassen für diese Primzahl siebend wirken. Allgemein entnehmen wir der Tabelle den folgenden Siebalgorithmus:

1. Schreibe die ersten n natürlichen Zahlen auf.
2. Bilde die Primzahlmenge $\mathcal{P} = \{5, 7, \dots, p_\rho\}$, wobei p_ρ die größte Primzahl $\leq \sqrt{6n+1}$ ist.
3. Berechne $\kappa(p)$ für alle $p \in \mathcal{P}$ und streiche alle Zahlen ν mit
$$\nu \equiv \pm\kappa(p) \bmod p \text{ für } \nu = 1, \dots, n.$$

In der Tabelle wurden die siebenden Restklassen mit Kreuzen angedeutet. Nach der Durchführung des obigen Siebalgorithmus bleiben alle ν übrig, für die $(6\nu - 1, 6\nu + 1)$ 2-Zwillinge sind, die keine der Primzahlen aus $\mathcal{P}$ enthalten. In anderen Worten gilt $p_\rho < 6\nu - 1 < 6\nu + 1 \leq 6n + 1$ für alle diese ν.

Die aus der Tabelle gewonnene Siebkonstruktion formulieren wir ein wenig um in dem

Lemma 2.1.1 *Die Zahlen $a_\nu = 36\nu^2 - 1$ sind genau dann durch ein $t \in \mathbb{N}_6$ teilbar, $t \neq 1$, falls für alle $p|t$ die Zahl ν in eine der Restklassen $+\kappa(p)$ oder $-\kappa(p)$ mod p fällt.*

Beweis: Sei t ein beliebiger nicht trivialer Teiler von $36\nu^2 - 1$ und $t = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ die Primzahlzerlegung von t. Wegen der Teilergeschlossenheit von $\mathbb{N}_6$ und $36\nu^2 - 1 \in \mathbb{N}_6$ ist auch $t \in \mathbb{N}_6$ und somit auch $p_i^{\alpha_i} \in \mathbb{N}_6$. In anderen Worten können Gleichungen der Form $p_i^{\alpha_i} = 6\kappa(p_i^{\alpha_i}) \pm 1$, $i = 1, \dots, k$ aufgestellt werden. Dies bedeutet aber, daß $\kappa(p_i^{\alpha_i})$ bzw. $-\kappa(p_i^{\alpha_i})$ invers zu 6

[7]Man sieht, das für alle $\nu \in \mathbb{Z}$ und $a \in [6\nu - 1, 6(\nu+1) - 1[$ der Wert von $\kappa(a)$ konstant gleich ν ist.

modulo $p_i^{\alpha_i}$ ist, falls $p_i^{\alpha_i}$ die Darstellung $6\kappa(p_i^{\alpha_i}) - 1$ bzw. $6\kappa(p_i^{\alpha_i}) + 1$ hat, $i = 1, \ldots, k$.

Die Bedingung $t|36\nu^2 - 1$ ist mit $36\nu^2 \equiv 1 \bmod p_i^{\alpha_i}$ für $i = 1, \ldots, k$ äquivalent, was z.B. aus dem Chinesischen Restsatz sofort folgt. Nach dem oben Gesagten können diese Kongruenzen vereinfacht werden zu $\nu^2 \equiv \kappa^2(p_i^{\alpha_i}) \bmod p_i^{\alpha_i}$. Dies ist gleichbedeutend mit

$$(\nu - \kappa(p_i^{\alpha_i}))(\nu + \kappa(p_i^{\alpha_i})) \equiv 0 \bmod p_i^{\alpha_i}, \qquad i = 1, \ldots, k.$$

Da $\mathbb{Z}_{p_i^{\alpha_i}}$ für $\alpha_i \geq 1$ ein Körper ist, passiert das genau dann, wenn $\nu \equiv +\kappa(p_i^{\alpha_i})$ oder $\nu \equiv -\kappa(p_i^{\alpha_i}) \bmod p_i^{\alpha_i}$ ist. Da t ein beliebiger Teiler war, gilt das auch für quadratfreie t, woraus die Behauptung folgt.

□

2.2 Anmerkungen zu Siebkonstruktionen

Wie wir im Abschnitt 2.1 gesehen haben, kann man ein siebtheoretisches Problem (z.B. das PZd-Problem) mit verschiedenen Siebkonstruktionen modellieren. Dabei ist das Siebproblem aus der Definition 1.3.2 abhängig von der Wahl des Polynoms h und der Primzahlmenge $\mathcal{P}$, das PZd-Problem hingegen ist es nicht, da es offenbar unterschiedliche Wahlen von h und $\mathcal{P}$ zuläßt. Offenbar kann man also einem siebtheoretischen Problem eine ganze Klasse von Siebkonstruktionen zuordnen, was nun formal geschehen soll.

In Anlehnung an die Siebdefinition 1.3.1 sei dem siebtheoretischen Problem Ω stets die Klasse S_Ω aller Tupel $(\mathcal{A}, \mathcal{P}, \mathcal{R})$ zugeordnet, deren Siebkonstruktionen $S(\mathcal{A}, \mathcal{P}, \mathcal{R})$ das Problem Ω modellieren. Der Begriff des "Modellierens" muß präzisiert werden. Wir betrachten eine uns bezüglich des Problems Ω interessierende geordnete, nicht unbedingt unendliche Teilmenge $\mathbb{N}_\Omega \subset \mathbb{N} = \{n_1 < n_2 < \cdots\}$ der natürlichen Zahlen. Das Problem Ω besteht darin, zu jedem $M \in \mathbb{N}$ möglichst genau die Anzahl der $n_i \in \mathbb{N}_\Omega$ mit $n_i \leq M$ abzuschätzen. Sei nun $\mathcal{A}$ eine geordnete Menge der Mächtigkeit N (vgl. Definition auf Seite 12) und $\mathcal{A}'$ die nach dem Sieben mit $\mathcal{P}$ und $\mathcal{R}$ verbliebene Teilmenge $\mathcal{A}' \subset \mathcal{A}$. Wir sagen, $S(\mathcal{A}, \mathcal{P}, \mathcal{R})$ **modelliert** das Siebproblem Ω, falls die folgenden Bedingungen erfüllt sind:

1. Es handelt sich um ein echtes Sieb, insbesondere gilt also $\mathcal{A}' \neq \emptyset$ und $\mathcal{A}' \neq \mathcal{A}$, ferner hängt die Mächtigkeit der Menge $\mathcal{A}'' = \mathcal{A} \backslash \mathcal{A}'$ nur von der Wahl von $\mathcal{P}$ und $\mathcal{R}$ ab.

2. Es gibt nur ein von $\mathcal{A}$ abhängiges M und nur von $\mathcal{P}$ und $\mathcal{R}$ abhängiges m mit $0 \leq m < M$, so daß die Menge $\mathbb{N}'_\Omega := \{n \in \mathbb{N}_\Omega, m < n \leq M\}$ nicht leer ist.

3. Es gibt eine bijektive Abbildung $\xi : \mathcal{A}' \to \mathbb{N}'_\Omega$. Insbesondere sind also $\mathcal{A}'$ und $\mathbb{N}'_\Omega$ gleich mächtig und ihre Mächtigkeit beträgt $N - |\mathcal{A}''|$.

Unser S_Ω besteht nun aus allen das Problem Ω modellierenden Siebkonstruktionen $S(\mathcal{A}, \mathcal{P}, \mathcal{R})$. Unser Fall $\Omega =$ *"PZd-Problem"* ist insofern atypisch, da wir nicht wissen, ob überhaupt unendlich viele d-Zwillinge existieren. Unser $\mathbb{N}_\Omega$ könnte sich also auch als endlich erweisen. Dennoch können wir viele Folgen $\mathcal{A}$ angeben, die alle, oder fast alle Primzahlzwillinge enthalten oder Produkte aus solchen sind[8]. Bis jetzt schienen dafür lediglich die Werte eines Polynoms zweiten Grades $h(n) = h_1(n)h_2(n)$ in Frage zu kommen mit zwei linearen Polynomen $h_1(n) = a_1n + b_1$, $h_2(n) = a_2n + b_2$, $a_1, a_2 \neq 0$. Es ist aber möglich, Polynome ersten Grades anzugeben, die zu S_Ω gehören. Man betrachte etwa das Polynom $h(n) = 6n - 1$. Es enthält alle Werte von $36n^2 - 1 = 6(6n^2) - 1$. Man könnte es noch weiter treiben und $h(n) = 2n - 1$ oder sogar $h(n) = n$ setzen. Jede neue Wahl von h zieht Veränderungen in der Wahl der siebenden Primzahlmenge $\mathcal{P}$ und der ihr zugeordneten Restklassenmenge $\mathcal{R}$ nach sich. Beispielsweise würde die Wahl $h(n) = n$, $\mathcal{P} = \mathbb{P}_6$ und $\mathcal{R} = \{\pm\kappa(p) \bmod p,\ p \in \mathcal{P}\}$ nach Lemma 2.1.1 gleichermaßen das PZ2-Problem im Sinne der obigen Definition modellieren wie das entsprechende Pendant mit $h(n) = 36n^2 - 1$, $\mathcal{P} = \mathbb{P}$ und $\mathcal{R} = \{0 \bmod p,\ p \in \mathcal{P}\}$.

Nach so vielen Beispielen von ein und dasselbe Problem modellierenden Siebkonstruktionen drängt sich sofort die Frage auf, ob man S_Ω für ein gegebenes Ω überhaupt vollständig angeben kann? Es gibt sehr viele Polynome, die das PZ2-Problem modellieren. Beispielsweise könnte man statt $h(n) = 36n^2 - 1$ auch jedes der Polynome $h_k(n) = (36n^2 - 1)^k$, $k \geq 1$ heranziehen mit denselben Mengen $\mathcal{P} = \mathbb{P}$ und $\mathcal{R} = \{0 \bmod p,\ p \in \mathcal{P}\}$. Die Mächtigkeit der gesiebten Menge gegenüber dem bereits behandelten Fall $k = 1$ würde sich natürlich nicht verändern und somit könnte man auch eine zählende bijektive Abbildung ξ zwischen den ungesiebten Werten von $h_k(n)$ und den zugehörigen Primzahlzwillingen angeben.

Nach Meinung des Verfassers ist das Problem der vollständigen Angabe von S_Ω und somit der systematischen Konstruktion von geeigneten Sieben

[8]Diese Einschränkungen ergeben sich aus der Notwendigkeit der Wahl eines geeigneten zählenden ξ.

für ein Problem Ω in der Literatur noch nicht aufgestellt worden. Obwohl es interessant ist, ist es nicht Gegenstand dieser Arbeit und wurde hier nicht weiter behandelt.

Wie wir gesehen haben, konnte man für das PZ2-Problem ein "effizientes" Polynom $h(n) = 36n^2 - 1$ angeben, das in bezug auf die Anzahl der beim Sieben gefundenen Zwillinge pro Polynomwerte besser als andere Polynome abgeschnitten hat. Um ähnliche "effiziente" Polynome für das allgemeine PZd-Problem aufzustellen, stelle man sich zuerst ein rechteckiges Zahlenschema $A = (a_{ij})$ vor mit den Einträgen

$$a_{ij} = 6i + 1 - (6j - 1), \qquad i, j \in \mathbb{N}_0,$$

wie in der Tabelle 2.2 angedeutet.

$a \backslash b$	5	11	17	23	$\cdots$
7	2	-4	-10	-16	$\cdots$
13	8	2	- 4	-10	$\cdots$
19	14	8	2	-4	$\cdots$
25	20	14	8	2	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Tabelle 2.2: Ein Zahlenschema, in dem in jeder Diagonalen der Abstand d von d-Zwillingen eingetragen ist. Alle d-Zwillinge mit $6 \nmid d$ sind hier vertreten.

Betrachtet man die Diagonalen dieser Matrix, so enthält die gesamte (unendliche) Matrix A alle geraden Zahlen $|d|$ mit $6 \nmid |d|$. Ferner treffen in jeder Diagonalen die Zahlen $(a, b) = (6i + 1, 6i - d + 1)$ aufeinander mit $a \equiv +1(6)$ und $b \equiv -1(6)$. In den jeweiligen Zeilen- und Spaltenüberschriften sieht man auch, daß diese beiden Progressionen ohne Ausnahme (natürlich bezogen auf Restklassenrepräsentanten im Bereich der natürlichen Zahlen für beide Progressionen) vertreten sind. Nach den Ausführungen zum Polynom $36\nu^2 - 1$ des letzten Abschnitts wissen wir aber, daß für jede Primzahl $p > 3$ in der Matrix A genau eine Zeile steht, wenn $p \equiv +1(6)$, und eine Spalte, falls $p \equiv -1(6)$ gilt. Somit treffen sich auf den Diagonalen fast alle[9] d-Zwillinge

[9] Genauer bis auf die Ausnahmen am Anfang, für die die Zahl $6n - d + 1$ noch negativ bleibt, oder für $d = 2$ den 2-Zwilling $(3, 5)$.

mit $6 \nmid d$. Offenbar kann man für die Polynome

$$h_d(n) := (6n+1)(6n-d+1)$$

jeweils geeignete Abbildungen κ_d definieren, mit denen sich für $6 \nmid d$ ähnlich effiziente Siebe wie im vierten Beispiel des vorigen Abschnitts konstruieren lassen. Auf die Herleitung dieser Abbildungen wurde hier (bis auf den bereits behandelten Fall $d = 2$) verzichtet.

Eine triviale, aber leicht zu übersehende, Tatsache, die man an der Matrix A auch sofort sehen kann, besteht darin, daß für alle d-Zwillinge $(p, p+|d|)$ mit $|d| \equiv 4(6)$ stets die kleinere Primzahl p in der Restklasse $+1(6)$ und die größere Primzahl $p+|d|$ in der Restklasse $-1(6)$ zu liegen kommt. Genau umgekehrt verhält es sich für alle d-Zwillinge $p, p+|d|$ mit $|d| \equiv 2(6)$. Deshalb bringen die Fälle mit $6|d$, $d \neq 0$ eine gewisse Schwierigkeit mit sich. Hier scheint die Wahl eines Polynoms wie $(6n+1)(6n-d+1)$ für $6|d$, etwa $d = 6$, nicht sinnvoll zu sein, da man so nur Primzahlen aus der Progression $+1(6)$ treffen würde. Ähnliche Schwierigkeiten bringt das Polynom $(6n-1)(6n-d-1)$ mit sich. Zwar konnte schon Dirichlet 1837 beweisen, daß eine arithmetische Progression wie $6n-1$, $n \in \mathbb{N}$ unendlich viele Primzahlen enthält[10], aber man konnte bis heute zusammen mit der Zwillingsvermutung auch nicht beweisen, daß es unendlich viele 6-Zwillinge vom Typ $(6n-1, 6n-6-1)$ gibt. Nun könnte es aber sein, daß die 6-Zwillingsvermutung insofern richtig ist, daß es zwar unendlich viele 6-Zwillinge vom Typ $(6n+1, 6n-6+1)$ aber nur endlich viele 6-Zwillinge vom Typ $(6n-1, 6n-6-1)$ gibt, und unser Polynom $(6n+1)(6n-6+1)$ würde nur endlich viele Ausnahmen nicht berücksichtigen. Eine derart ungleiche Verteilung der Primzahlen in den Progressionen $6n-1$ und $6n+1$ scheint aber unwahrscheinlich zu sein. Denn der 1899 von De La Vallée-Poussin bewiesene sog. **Primzahlsatz für arithmetische Progressionen** sagt aus, daß jede Progression $nq+k$, mit $\mathrm{ggT}(q,k) = 1$ und $n \in \mathbb{N}$ die folgende Anzahl an Primzahlen enthält:

$$\pi(x,q,k) := \sum_{\substack{p \leq x \\ p \equiv k \bmod q}} 1 = \frac{1}{\phi(q)}\, li\ x + \mathcal{O}\left(xe^{-c\sqrt{\log x}}\right). \tag{2.1}$$

Dabei hängt die positive Konstante c nur von q ab. Für $\phi(6) = 2$ gibt es also etwa (asymptotisch) gleich viele Primzahlen $p \equiv -1(6)$ und $p \equiv +1(6)$

[10]Genauer hat er gezeigt, daß alle Progressionen $nq+k$ mit $\mathrm{ggT}(q,k) = 1$, $n \in \mathbb{N}$ unendlich viele Primzahlen enthalten, vgl. Dirichlet [15]

mit $p < x$, obwohl hier natürlich nichts über die Abstände dieser Primzahlen zueinander ausgesagt wird[11].

Wenn man annimmt, daß auch die Verteilungen der Abstände zwischen zwei Primzahlen in den beiden Progressionen $6n \pm 1$ nicht wesentlich voneinander abweichen, muß man schlußfolgern, daß es etwa doppelt so viele d-Zwillinge mit $6|d$ gibt als d'-Zwillinge mit $6 \nmid d'$, wenn d und d' nur wenig voneinander abweichen.

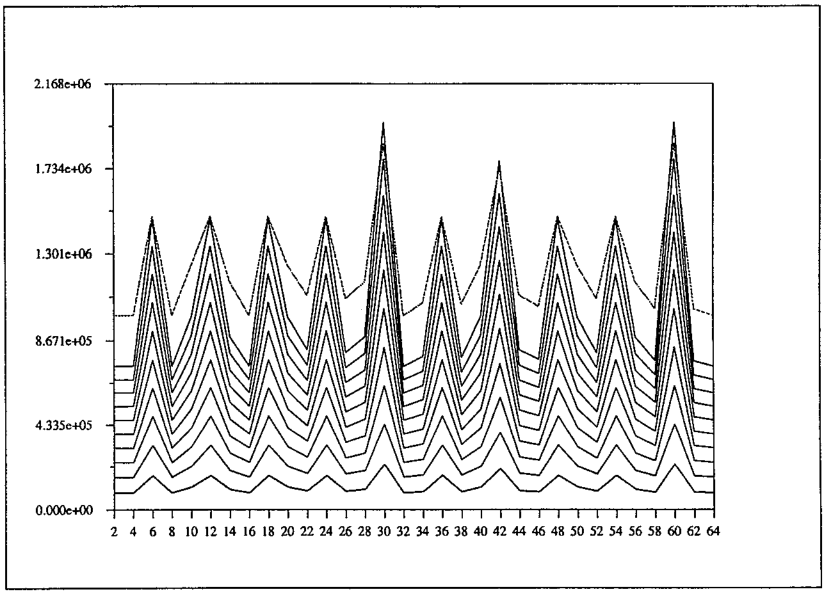

Abbildung 2.1: Gezählt wurden die Häufigkeiten der Zwillinge $(p, p+d)$, wenn p die k-millionste Primzahl, $k = 1, \ldots, 10$ durchläuft (Linien von unten nach oben). Die oberste Linie verbindet die Werte der 3. Spalte der Tabelle 2.3.

Um diese These zu veranschaulichen, wurden vom Verfasser für die geraden Werte $d = 2, \ldots, 64$ die Häufigkeiten der d-Zwillinge $(p, p+d)$ für die ersten 10 Millionen Primzahlen p gezählt und das Ergebnis in der Abb. 2.1 zusammengefaßt. Jede der 10 Linien steht dabei für die Häufigkeiten der d-Zwillinge bis $(p, p+d)$, wenn p die k-millionste Primzahl durchläuft für

[11]Die Funktion $li\ x$ - der "logarithmus integralis von x"- hat den Wert des Integrals $\int_2^x \frac{du}{\log u} + li\ 2$ mit $li\ 2 = 1.04\ldots$

$k = 1, \dots, 10$. Diese Primzahlen waren im einzelnen:

$$15485863, 32452843, 49979687, 67867967, 86028121,$$
$$104395301, 122949823, 141650939, 160481183, 179424673.$$

Man sieht nicht nur, daß die obige These bestätigt wird, sondern auch, daß die Zahlen $\pi_d(n)$ nicht so sehr davon abhängen, wie groß d ist, sondern davon, welche Primteiler d hat. Die Werte für $d = 2, 4, 8, 16, 32, 64$ bleiben beispielsweise auf dergleichen Höhe. Ebenso die Werte für $d = 10, 20, 50$ oder $d = 6, 12, 18, 24, 36, 48, 54$. Darüber hinaus scheint π_d größer auszufallen, falls d von 6 und mindestens einer der Primzahlen $p > 3$ geteilt wird. Ist die wahre Größenordnung der d-Zwillinge tatsächlich

$$\pi_d(N) \overset{!}{\sim} c_d \frac{N}{\log^2 N},$$

mit einer von d abhängigen Konstanten c_d, dann scheint in dieser Konstanten der Wert von $d/\phi(d)$ eine Rolle zu spielen, wie auch schon im Satz 1.7.2.

In der Tabelle 2.3 wurde die Formel (1.46) mit der zehnmillinonsten Primzahl $p = 179424673$ ohne die Konstante $c(2)$ getestet. Man sieht dort, daß die Konstante $c(2)$ nicht viel größer als 1 zu sein braucht, um eine gute obere Schranke für $\pi_d(x)$ zu liefern.

Zum Schluß dieses Abschnitts kehren wir nochmals zur Hardy-Littlewoodschen Vermutung (1.1) zurück. Außer der dort definierten Konstanten $C_2 = 0.66016\dots$ vor dem Bruch $x/log^2 x$ vermuteten sie noch einen Korrekturfaktor

$$J(d) := \prod_{p|d,\ p>2} \frac{p-1}{p-2}.$$

Mit diesem Korrekturfaktor und der Konstanten C_2 wurde in der Tabelle 2.4 (Seite 65) die Genauigkeit der Hardy-Littlewoodsche Vermutung getestet. Man sieht dort, daß der Korrekturterm ziemlich genau die Oszillationen der Häufigkeiten der gezählten d-Zwillinge mitmacht.

2.3 Untere Schranke für $\pi_2(n)$?

Um im vorab viele lange Wortwiederholungen zu vermeiden, ist es sinnvoll, die folgenden Abkürzungen einzuführen:
Seien $k, m \in \mathbb{N}$. Dann nennen wir das Paar $(6k-1, 6k+1)$ ein

d	$\pi_d(p+d)$	$\frac{d}{\phi(d)}p/\log^2 p$	Quot.	d	$\pi_d(p+d)$	$\frac{d}{\phi(d)}p/\log^2 p$	Quot.
2	738597	993492	0.74	34	787932	1055585	0.75
4	738718	993492	0.74	36	1478412	1490238	0.99
6	1477321	1490238	0.99	38	782068	1048686	0.75
8	738005	993492	0.74	40	985086	1241865	0.79
10	984809	1241865	0.79	42	1773231	1738611	1.02
12	1477496	1490238	0.99	44	820919	1092841	0.75
14	887143	1159074	0.77	46	773523	1038650	0.74
16	738949	993493	0.74	48	1477835	1490238	0.99
18	1478551	1490238	0.99	50	984903	1241865	0.79
20	984159	1241865	0.79	52	805508	1076283	0.75
22	821020	1092841	0.75	54	1478523	1490238	0.99
24	1479600	1490238	0.99	56	885662	1159074	0.76
26	806236	1076283	0.75	58	766582	1028974	0.74
28	886949	1159074	0.77	60	1970570	1862797	1.06
30	1970048	1862797	1.06	62	764662	1026608	0.74
32	737668	993492	0.74	64	738835	993492	0.74

Tabelle 2.3: Statistik der d-Zwillinge im Vergleich zur oberen Schranke des Satzes 1.7.2 für die 10000000-ste Primzahl $p = 179424673$ ohne die dortige Konstante $c(2)$. In der vierten Spalte befinden sich die Quotienten $\phi(d)\pi_d(p+d)\log^2 p/(dp)$. Zum optischen Vergleich wurden die Werte der dritten Spalte in der Abbildung 2.1 als gestrichelte Linie eingezeichnet.

- *cc*-Paar, falls $6k-1$ und $6k+1$ beide gleichzeitig zusammengesetzt sind;
- *pp*-Paar, falls $6k-1$ und $6k+1$ beide prim (also 2-Zwillinge) sind. Analog sprechen wir auch von *cp*- bzw. *pc*-Paaren, wenn nur $6k-1$ bzw. nur $6k+1$ zusammengesetzt ist;
- 00_m-Paar, falls sowohl $6k-1$ also auch $6k+1$ zu m nicht teilerfremd sind, also wenn $\mathrm{ggT}(6k-1,m) > 1$ und $\mathrm{ggT}(6k+1,m) > 1$ ist;
- 11_m-Paar, falls $\mathrm{ggT}(6k-1,m) = 1$ und gleichzeitig $\mathrm{ggT}(6k+1,m) = 1$ ist. Auch hier sind entsprechend zu verstehende Mischformen 01_m bzw. 10_m möglich. Falls es unzweideutig ist, benutzen wir für 11_m-, 10_m-, 01_m- bzw. 00_m-Paare einfach die Kurzformen 11-, 10-, 01- bzw. 00-Paare.

d	$\pi_d(p+d)$	$HL(p,d)$	Quot.	d	$\pi_d(p+d)$	$HL(p,d)$	Quot.
2	738597	655863	1.126	34	787932	699588	1.126
4	738718	655863	1.126	36	1478412	1311727	1.127
6	1477321	1311727	1.126	38	782068	694444	1.126
8	738005	655863	1.125	40	985086	874485	1.126
10	984809	874485	1.126	42	1773231	1574072	1.127
12	1477496	1311727	1.126	44	820919	728737	1.126
14	887143	787036	1.127	46	773523	687095	1.126
16	738949	655863	1.127	48	1477835	1311727	1.127
18	1478551	1311727	1.127	50	984903	874485	1.126
20	984159	874485	1.125	52	805508	715487	1.126
22	821020	728737	1.127	54	1478523	1311727	1.127
24	1479600	1311727	1.128	56	885662	787036	1.125
26	806236	715487	1.127	58	766582	680155	1.127
28	886949	787036	1.127	60	1970570	1748969	1.127
30	1970048	1748969	1.126	62	764662	678479	1.127
32	737668	655863	1.125	64	738835	655863	1.127

Tabelle 2.4: Häufigkeiten der d-Zwillinge im Vergleich zur Hardy-Littlewoodschen Vermutung (1.1), die den asymptotischen Wert $HL(p,d) := 2C_2J(d)x/\log^2 x$ mit $J(d) := \prod_{p|d,\ p>2} \frac{p-1}{p-2}$ und der Konstanten $C_2 = 0.66061\ldots$ vorhersagt. Berechnet wurde der Wert für $x = 179424673$. Auffällig ist der fast konstante Quotient der beiden Werte.

Sei nun $n \in \mathbb{N}$ und $\mathcal{B}$ die Menge der Paare $(6k-1, 6k+1)$, $k = 1, \ldots, n$. In $\mathcal{B}$ lassen sich nun drei disjunkte Klassen von Paaren ausmachen:

$$\mathcal{B}_{cc} := \text{Menge aller } cc\text{-Paare in } \mathcal{B},$$

$$\mathcal{B}_{pp} := \text{Menge aller } pp\text{-Paare in } \mathcal{B},$$

$$\mathcal{B}_{xx} := \mathcal{B} \setminus (\mathcal{B}_{cc} \cup \mathcal{B}_{pp}).$$

Seien als nächstes $\mathcal{B}(n), \mathcal{B}_{cc}(n), \mathcal{B}_{pp}(n)$ und $\mathcal{B}_{xx}(n)$ die Anzahlen der Paare in den jeweiligen Mengen. Da wir uns besonders für $\mathcal{B}_{pp}(n)$ interessieren, wollen wir die drei Zahlen zueinander in Beziehung setzen. Dazu führen wir für alle $k \in \mathbb{N}$ die charakteristischen Funktionen ein:

$$g^+(k) := \begin{cases} 1, & \text{falls } 6k+1 \text{ prim ist,} \\ 0, & \text{sonst.} \end{cases}$$

$$g^-(k) := \begin{cases} 1, & \text{falls } 6k-1 \text{ prim ist,} \\ 0, & \text{sonst.} \end{cases}$$

$$g^0(k) := g^+(k) \cdot g^-(k).$$

Man beachte, daß $g^0(k)$ genau dann 1 ist, wenn $(6k-1, 6k+1)$ ein *pp*-Paar also ein 2-Zwilling ist. Damit gilt für $\mathcal{B}_{pp}(n)$:

$$\begin{aligned} B_{pp}(n) &= \pi_2(6n+1) - 1 = \sum_{k=1}^{n} g^0(k) = \sum_{k=1}^{n} g^+(k) g^-(k) \\ &= \underbrace{\sum_{k=1}^{n} g^+(k) + \sum_{k=1}^{n} g^-(k)}_{=\pi(6n+1)-2} - n + \underbrace{\sum_{k=1}^{n} (1 - g^-(k))(1 - g^+(k))}_{=\mathcal{B}_{cc}(n)}. \end{aligned}$$

Damit folgt die für alle $n \in \mathbb{N}$ gültige Beziehung

$$\pi_2(6n+1) + 1 = \pi(6n+1) - n + \mathcal{B}_{cc}(n), \tag{2.2}$$

die die Anzahl der 2-Zwillinge in Zusammenhang mit der Anzahl aller Primzahlen und aller *cc*-Paare bringt[12].

Man könnte nun denken, daß dies der Schlüssel zur Lösung des PZ2-Problems sei: Man finde eine wachsende Funktion, die eine untere Schranke für $\mathcal{B}_{cc}$ darstellt, setze sie in die Gleichung (2.2) ein und, vorausgesetzt die Funktion wächst schnell genug, kompensiert sie mit den anderen Gliedern den Term $-n$, so daß wir eine wachsende Funktion als untere Schranke für $\pi_2(6n+1)$ erhalten.

Doch diese Denkweise weckt illusorische Hoffnungen, denn wir wissen bereits aus dem Satz 1.1.7.2, daß es für $x = 6n+1$ nicht mehr als $cx/log^2 x$ 2-Zwillinge geben kann. Es war ebenfalls De La Vallée Poussin, der zeigte, daß für die Anzahl der Primzahlen $\leq x$ asymptotisch gilt[13]

$$\pi(x) = \sum_{p \leq x} 1 \sim \frac{x}{\log x}. \tag{2.3}$$

[12]Die Gleichung (2.2) ist relativ trivial und wurde auch in anderen Formen aufgestellt, die z.B. die Zahl $\mathcal{B}_{xx}$ enthalten, vgl. Jean-Pierre Bauer [4].

[13]Genauer zeigte er, daß $\pi(x) = li\ x + \mathcal{O}\left(x \exp(-c\sqrt{\log x})\right)$ gilt mit einer von x unabhängigen Konstanten $c > 0$. Durch m-mal fortgesetzte partielle Integration erhält man die für $x \to \infty$ asymtotische Formel

$$li\ x = \frac{x}{\log x} + \frac{x}{\log^2 x} + \cdots + \frac{(m-1)!x}{\log^m x} + \mathcal{O}\left(m! \frac{x}{\log^{m+1} x}\right).$$

Selbst wenn es uns also gelingen würde, eine untere Schranke für $\mathcal{B}_{cc}$ zu finden, dürften wir den Term $\pi(x)$ nicht als "Fehlerglied" auffassen, denn dieses wäre asymptotisch größer als unsere untere Schranke jemals werden kann. Vielmehr müßten wir jedes Primzahlvorkommen, das in $\pi(x)$ einmal gezählt wird, einzeln, z.B. aufgrund wie auch immer gearteter kombinatorischer Überlegungen, mit einem in $\mathcal{B}_{cc}((x-1)/6)$ gezählten cc-Paar "verrechnen". So etwas käme aber einer Formel für Primzahlen gleich, die höchstwahrscheinlich niemals gefunden wird[14].

Trotz dieser schlechten Aussichten wurde hier die Zahl $\mathcal{B}_{cc}(n)$ näher untersucht. Die Ergebnisse dieses Studiums sollen nun vorgestellt werden.

2.4 Eine untere Schranke für $\mathcal{B}_{cc}(n)$

Mit dem Primzahlsatz und einfachen kombinatorischen Überlegungen findet man eine schlechte obere und eine relativ gute untere Schranke für $\mathcal{B}_{cc}(n)$. Obwohl uns das, wie schon erwähnt, bei der Behandlung der Gleichung (2.2) nicht weiterbringt, ist das folgende Ergebnis nichttrivial und dem Verfasser aus der Literatur nicht bekannt.

Satz 2.4.1 *Setzt man, $x = 6n + 1$ so gibt es von x unabhängige positive Konstanten c, und c', so daß für genügend großes n gilt:*

$$\frac{x-1}{6} - li\ x \leq \mathcal{B}_{cc}(n) + \mathcal{O}\left(xe^{-c'\sqrt{\log x}}\right) \leq \frac{x-1}{6} - li\ x + c\frac{x}{\log^2 x}$$

Beweis: Die Mengen $\mathcal{B}_{cc}$, $\mathcal{B}_{pp}$ und $\mathcal{B}_{xx}$ sind disjunkt, so daß gilt

$$\mathcal{B}_{cc}(n) = n - \mathcal{B}_{xx}(n) - \mathcal{B}_{pp}(n), \qquad \forall\ n \in \mathbb{N}.$$

Nach dem Primzahlsatz für arithmetische Progressionen gibt es eine von x unabhängige Konstante c', so daß gilt

$$\mathcal{B}_{xx}((x-1)/6) + \mathcal{B}_{pp}((x-1)/6) = \frac{li\ x}{2} + \mathcal{O}\left(xe^{-c'\sqrt{\log x}}\right). \tag{2.4}$$

[14] Es gibt aber Primzahlformeln, die gewissermaßen die Primzahlen aus sich selbst heraus erzeugen: Ist nach Sierpiński p_n die n-te Primzahl und $\alpha := \sum p_n 10^{-2^n}$, dann gilt $p_n = \lfloor 10^{2^n}\alpha \rfloor - 10^{2^{n-1}} \lfloor 10^{2^{n-1}} \alpha \rfloor$, vgl [38]. Man beachte, daß man trotz der Richtigkeit dieser Aussage sehr viele Primzahlen, insbesondere auch p_n, schon vorher kennen muß, um die Zahl α mit ausreichender Genauigkeit zu berechnen.

Bis auf die Primzahlen 2 und 3 kommen alle restlichen $\pi(x)-2$ Primzahlen in den Progressionen $6n-1$ und $6n+1$, mal in pp-, mal in pc- oder cp-Paaren vor. Dabei gilt nach dem Schubfachprinzip: Je mehr pc- und cp-Paare es gibt, desto weniger (bei bekanntem asymptotischem Wachstum von $\pi(x)$) "Platz" bleibt zur Entstehung von pp- und cc-Paaren. Umgekehrt muß es mehr pp- und cc-Paare geben, wenn asymptotisch weniger pc- und cp-Paare vorkommen[15].

Man stelle sich nun die Matrix $A = (a_{ij}) \in \mathbb{N}^{n,n}$ vor mit $a_{ij} = (6i+1)(6j-1)$ für $i,j = 1,\ldots,n$. In jeder Spalte bzw. jeder Zeile dieser Matrix gibt es asymptotisch für $n \to \infty$ die gleiche Anzahl an Primzahlen p und q des Typs $p = 6j-1$ und $q = 6i+1$.

Gibt es unendlich viele Primzahlzwillinge, dann wissen wir nach dem Satz 1.1.7.2, daß maximal $cx/\log^2 x$ solche bis x existieren können, mit einer von x unabhängigen positiven Konstanten c, und so bleiben dann mindestens

$$\frac{li\ x}{2} - c\frac{x}{\log^2 x} + \mathcal{O}\left(xe^{-c'\sqrt{\log x}}\right)$$

viele Primzahlen p in der Progression $6j-1$ und ebensoviele Primzahlen q in der Progression $6i+1$ übrig. Sie können per definitionem nur noch pc- oder cp-Paare bilden. In der Matrix A bleiben noch

$$\frac{x-1}{6} - c\frac{x}{\log^2 x}$$

Zahlen a_{ii} auf der Diagonalen, die nicht Produkte von 2 Primzahlen sind. Davon muß noch die doppelte Anzahl der restlichen Primzahlen in beiden Progressionen abgezogen werden, und es folgt

$$\mathcal{B}_{cc}(n) \le \frac{x-1}{6} - c\frac{x}{\log^2 x} - 2\left(\frac{li\ x}{2} - c\frac{x}{\log^2 x} + \mathcal{O}\left(xe^{-c'\sqrt{\log x}}\right)\right)$$

und daraus die rechte Ungleichung. Die untere Schranke erhält man, wenn man annimmt, daß es nur endlich viele 2-Zwillinge gibt und somit $\mathcal{B}_{pp}(n)$ für $n \to \infty$ eine Konstante ist. Dann bilden asymptotisch gesehen fast alle bis auf endlich viele Primzahlen Pärchen in $\mathcal{B}_{xx}$, und deshalb ist

$$\mathcal{B}_{cc}(n) \ge \frac{x-1}{6} - 2\left(\frac{li\ x}{2} + \mathcal{O}\left(xe^{-c'\sqrt{\log x}}\right)\right).$$

□

[15] Insofern, und das sah man schon anhand der Gleichung (2.2), nehmen $\mathcal{B}_{cc}(n)$ und $\mathcal{B}_{pp}(n)$ in dem Sinne zu (ab), in welchem $\mathcal{B}_{xx}(n)$ kleiner (größer) wird.

2.5 Kombinatorische Gesetze der Paarenbildung in $\mathcal{B}_{cc}$

Aus dem Ergebnis des Satzes 2.4.1 kann man eine asymptotische Formel der Form

$$\mathcal{B}_{cc}(n) = \frac{x-1}{6} - li\ x + \mathcal{O}\left(\frac{x}{\log^2 x}\right), \qquad x = 6n+1, n \to \infty$$

ableiten. Das Fehlerglied $\mathcal{O}\left(x/\log^2 x\right)$ absorbiert den Fehler[16] $\mathcal{O}\left(xe^{-c'\sqrt{\log x}}\right)$. Der neue Fehlerterm ist zu groß, um mit der Gleichung (2.2) ein brauchbares Ergebnis zu liefern. Wir müßten also etwas sorgfältiger vorgehen.

Ein Weg, dies zu tun, besteht darin, statt nach $\mathcal{B}_{cc}(n)$ für ein $N \in \mathbb{N}$ zuerst nach der Anzahl der 00_N-Paare zu fragen:

$$\mathcal{B}_{00}(n) \ := \ \#\{k : (6k-1, 6k+1) \text{ ist ein } 00_N - \text{Paar}, \ k = 1, \ldots, n\},$$

d.h. derjenigen Paare mit $\mathrm{ggT}(6k-1, N) > 1$ und $\mathrm{ggT}(6k+1, N) > 1$ für $k = 1, \ldots, n$. In diesem Abschnitt wird für $\mathcal{B}_{00}(n)$ eine Formel angegeben.

Definition 2.5.1 *Sei h ein ganzzahliges Polynom mit der Zerlegung*

$$h(\nu) = \prod_{i=1}^{r} h_i(\nu),$$

wobei die Polynome h_i alle irreduzibel über $\mathbb{Z}[X]$ sind. Wir setzen

$$\phi_h(n) \ := \ \#\{m : \ \mathrm{ggT}(n, h(m)) = 1, m = 1, \ldots, n\}$$

und

$$\begin{aligned}\Phi_h(n) \ := \ & \#\{(h_1(m), \ldots, h_r(m)) : \\ & \mathrm{ggT}(h_1(m), n) > 1 \ \wedge \cdots \wedge \ \mathrm{ggT}(h_r(m), n) > 1, \\ & m = 1, \ldots, n\}.\end{aligned}$$

[16] Tatsächlich gilt $\mathcal{O}\left(xe^{-c'\sqrt{\log x}}\right) = o\left(\frac{x}{\log^A x}\right)$ sogar für ein beliebig großes aber festes $A \geq 1$.

Insofern ist $\phi_h(n)$ die Verallgemeinerung der Eulerschen ϕ-Funktion wenn man $h(m) = m$ setzt. $\Phi_h(n)$ zählt alle m, $1 \le m \le n$, für die alle Polynomwerte der irreduziblen Polynome $h_1, \ldots, h_r$ zu n nicht teilerfremd sind.

Nach dem Lemma 1.1.3.1 gilt für jedes $n \in \mathbb{N}$ mit $h(\nu) = 36\nu^2 - 1$:

$$\phi_h(n) \;=\; \sum_{\nu \le n} \sum_{t \mid \mathrm{ggT}(h(\nu),n)} \mu(t) = \sum_{t \mid n} \mu(t) \sum_{\substack{\nu \le n \\ h(\nu) \equiv 0 \bmod t}} 1.$$

Wie wir gesehen haben, hat die Gleichung $h(\nu) \equiv 0 \bmod p$ für $p = 2, 3$ keine Lösungen, so daß die innere Summe für alle Teiler $t|n$ mit $\mathrm{ggT}(t, 6) > 1$ leer ist. Andererseits hat die Gleichung nach Lemma 2.1.1 jeweils zwei Lösungen $\pm\kappa(p) \bmod p$ für alle Primzahlen $p > 3$. Bezeichnen wir mit $\sigma(t)$ diese Anzahl, dann ist σ multiplikativ, und für Primzahlen gilt also

$$\sigma(p) = \begin{cases} 0, & \text{falls } p = 2, 3, \\ 2, & \text{falls } p > 3. \end{cases}$$

Unter den n Zahlen gibt es für jedes $t|n$ jeweils $n\sigma(t)/t$ Lösungen. Damit erhalten wir

$$\begin{aligned} \phi_h(n) \;&=\; n \sum_{t \mid n} \mu(t) \frac{\sigma(t)}{t} = n \sum_{\substack{t \mid n \\ \mathrm{ggT}(t,6) > 1}} \mu(t) \frac{2^{\omega(t)}}{t} \\ &= n \prod_{\substack{p \mid n \\ p > 3}} \left(1 - \frac{2}{p}\right). \end{aligned} \tag{2.5}$$

für jedes $n \in \mathbb{N}$. Z.B. ist nun $\phi(60) = 60(1 - 2/5) = 36$ die Anzahl der Werte von $36\nu^2 - 1$ mit $\mathrm{ggT}(36\nu^2 - 1, 60) = 1$ für $\nu = 1, \ldots, 60$. Wir bemerken auch, daß $\phi_h(n)$ wegen $\mathrm{ggT}(6\nu - 1, 6\nu + 1) = 1$ gleichzeitig (für jedes n) die Anzahl der 11_n-Paare zählt. Zum Beispiel gibt es genau $\phi_h(60) = 36$ Zahlenpaare $(6\nu - 1, 6\nu + 1)$, $\nu = 1, \ldots, 60$ mit $\mathrm{ggT}(6\nu - 1, 60) = 1$ und $\mathrm{ggT}(6\nu + 1, 60) = 1$.

Eine Formel für $\Phi_h(n)$, also die Anzahl der 00_n-Paare für $\nu = 1, \ldots, n$, wenn $h(\nu) = 36\nu^2 - 1$ gesetzt wird, ist nicht so leicht herzuleiten. Um die Sache ein wenig zu vereinfachen, kürzen wir $\Phi_h(n)$ mit Φ ab und betrachten zuerst nur die Fälle mit $n \in \mathbb{N}_6$. Anschließend werden wir die dafür gefundene Formel auf alle $n \in \mathbb{N}$ ausdehnen.

Man könnte zuerst vermuten, daß eine solche Formel rein kombinatorischer Natur sein wird, also nur von der Anzahl der Primzahlen und/oder davon abhängen wird, ob es verschiedene sind. Dem ist jedoch nicht so, denn die durch Auszählen erhaltenen Werte

$$\begin{aligned}
\Phi(5\cdot 7\cdot 11) &= 40\\
\Phi(5\cdot 7\cdot 7) &= 14\\
\Phi(5\cdot 7\cdot 13) &= 44\\
\Phi(7\cdot 7\cdot 13) &= 14\\
\Phi(7\cdot 7\cdot 7) &= 0
\end{aligned}$$

verraten uns, daß $\Phi(n)$ weder eine multiplikative Funktion ist, noch scheint sie nur von $\omega(n)$ oder nur von der Größe der Primzahlen abzuhängen, die n teilen. Es fällt auf, das für alle $p > 3$, $\alpha \geq 0$ gilt, daß $\Phi(p^\alpha) = 0$ ist, denn n muß ja wenigstens von 2 verschiedenen Primzahlen $p > 3$ teilbar sein, damit die eine in $6\nu - 1$ und gleichzeitig die andere in $6\nu + 1$ aufgeht.

Um der Lage Herr zu werden, nehmen wir also zuerst an, daß n quadratfrei ist und von ρ verschiedenen Primzahlen $p_1, \ldots, p_\rho > 3$ geteilt wird. Jedes Paar $(6\nu - 1, 6\nu + 1)$ für $\nu = 1, \ldots, n$ versehen wir mit einer ρ-stelligen "Signatur" $(\chi_1, \chi_2, \ldots, \chi_\rho)_\nu$ mit

$$\chi_r := \begin{cases} 1, & \text{falls } p_r | 6\nu + 1 \\ -1, & \text{falls } p_r | 6\nu - 1 \\ 0, & \text{falls } p_r \nmid 36\nu^2 - 1 \end{cases} \qquad \text{für } r = 1, \ldots, \rho.$$

Man beachte, daß nur einer der drei Fälle auf einmal eintreten kann, so daß diese Definition sinnvoll ist. Nun zeigen wir das folgende

Lemma 2.5.1 *Sei $n \in \mathbb{N}_6$ quadratfrei mit der Primzerlegung $n = p_1 \cdots p_\rho$. Sei t ein beliebiger Teiler von n mit der Primzerlegung $t = q_1 \cdots q_\tau$ mit $0 \leq \tau = \omega(t) \leq \rho$. Dann ist die Anzahl der Paare $(6\nu-1, 6\nu+1)$, $\nu = 1, \ldots, n$, für die gilt $\mathrm{ggT}(36\nu^2 - 1, t) = t$ und $\mathrm{ggT}(36\nu^2 - 1, n/t) = 1$, d.h. derjenigen, in denen alle Primteiler von t, aber keine Primteiler von (n/t) in $6\nu - 1$ und/oder in $6\nu + 1$ aufgehen, gleich $2^{\omega(t)}\phi_h(n/t)$.*

Beweis: Für $t = 1$ reduziert sich diese Aussage zu $\phi_h(n)$ als der Anzahl der Paare mit $\mathrm{ggT}(36\nu^2 - 1, n) = 1$, was aus der Gleichung (2.5) sofort folgt. Für $t > 1$ sei o.B.d.A. $t = p_1 \cdots p_\tau$.

Wir teilen zuerst den Bereich $1, \ldots, n$ in $d := n/t$ Intervalle auf:

$$\begin{array}{rcl} 1, & \ldots & , t \\ t+1, & \ldots & , 2t \\ \vdots & \vdots & \vdots \\ (d-1)t+1, & \ldots & , dt \end{array}.$$

In jedem der d Zeilen gibt es genau 2^τ Lösungen der Kongruenz

$$36\nu^2 - 1 \equiv 0 \mod t.$$

In anderen Worten gibt es genau 2^τ Signaturen des Typs

$$(\chi_1, \ldots, \chi_\rho)_\nu = (\underbrace{\pm 1, \ldots, \pm 1}_{\tau}, \chi_{\tau+1}, \ldots, \chi_\rho)$$

mit beliebigen Werten für $\chi_{\tau+1}, \ldots, \chi_\rho$. Die Bedingung $\mathrm{ggT}(36\nu^2 - 1, n/t) = 1$ macht aber Signaturen der Form

$$(\chi_1, \ldots, \chi_\rho)_\nu = (\underbrace{\pm 1, \ldots, \pm 1}_{\tau}, \underbrace{0, \ldots, 0}_{\rho-\tau}) \tag{2.6}$$

notwendig. Schreibt man das obige Schema etwas anders auf:

$$\begin{array}{rcl} 1, & \ldots & , d \\ d+1, & \ldots & , 2d \\ \vdots & \vdots & \vdots \\ (t-1)d+1, & \ldots & , td \end{array},$$

so folgt für jedes ν aus der i-ten Zeile und j-ten Spalte

$$36\nu^2 - 1 = 36(di + j)^2 - 1 = 36(d^2i^2 + 2dij + j^2) - 1 \equiv 36j^2 - 1 \mod d.$$

Somit gilt für jede der Primzahlen $p|d$ (also $p = p_r$ mit $r = \tau + 1, \ldots, \rho$)

$$p|36\nu^2 - 1 \iff p|36j^2 - 1.$$

Nach (2.5) gibt es nun genau $\phi_h(d)$ Spalten $j = 1, \ldots, d$ im zweiten Schema, wo die Bedingung $\mathrm{ggT}(36j^2 - 1, d) = 1$ erfüllt ist. Bezeichnen wir mit j' jede solche Spalte, dann folgt die Behauptung, wenn wir zeigen können, das es genau 2^τ Lösungen der Kongruenz

$$36(d^2i^2 + 2dij' + j'^2) - 1 \equiv 0 \mod t$$

für $i = 1, \ldots, t$ pro Spalte gibt.

Dies folgt aber daraus, daß wegen $\mathrm{ggT}(t,d) = 1$ mit i auch die Zahl $di+j'$ das gesamte Restsystem modulo t durchläuft.

□

Bemerkung: Aus dem Lemma 2.5.1 folgt die hübsche Formel

$$n = \sum_{t|n} 2^{\omega(t)} \phi_h\left(\frac{n}{t}\right), \qquad \forall\, n \in \mathbb{N}_6, \mu(n) \neq 0,$$

weil die Signaturen (2.6) für alle Teiler $t|n$ mit $\omega(t) = \tau$ stehen, und alle Signaturen für $\nu = 1, \dots, n$ disjunkt sind.

Lemma 2.5.2 *Seien die Bezeichnungen des Lemmas 2.5.1 beibehalten. Dann gibt es unter den* $2^\tau \phi_h(n/t)$ *Paaren mit* $\mathrm{ggT}(36\nu^2-1, n/t) = 1$ *und* $t|36\nu^2-1$ *genau* $(2^\tau - 2)\phi_h(n/t)$ *Paare vom Typ* 00_t*, also mit* $\mathrm{ggT}(6\nu-1, t) > 1$ *und* $\mathrm{ggT}(6\nu+1, t) > 1$*, wenn* $\tau \geq 2$*. Sonst gibt es keine solchen Paare.*

Beweis: Die Zusatzforderung an die $z = 2^\tau \phi_h(n/t)$ Paare, sie sollten vom Typ 00_t sein, bedeutet, daß nicht alle Primzahlen $q|t$ gemeinsam in $6\nu-1$ bzw. $6\nu+1$ aufgehen. Weil t quadratfrei ist, sind es die 2 Fälle $t|6\nu-1$ bzw. $t|6\nu+1$, die nun nicht mitgezählt werden dürfen und von z abgezogen werden müssen.

Ist $\tau < 2$, so ist $t = 1$ oder t ist eine Primzahl, und kann daher nicht gleichzeitig $6\nu-1$ und in $6\nu+1$ aufgehen und so ein 00_t-Paar erzeugen.

□

Nach diesen Vorbereitungen sind wir in der Lage, der Formel für Φ eine erste Gestalt zu geben:

Lemma 2.5.3 *Ist* $n \in \mathbb{N}_6$ *quadratfrei und Produkt von mindestens 2 verschiedenen Primzahlen* $n = p_1 \cdots p_\rho$, $\rho \geq 2$, *so gilt für* $h(\nu) = 36\nu^2 - 1$*:*

$$\begin{aligned} \Phi(n) &= (2^2-2) \sum_{1\leq i<j\leq\rho} \phi_h\left(\frac{n}{p_i p_j}\right) \\ &+ (2^3-2) \sum_{1\leq i<j<k\leq\rho} \phi_h\left(\frac{n}{p_i p_j p_k}\right) \\ &+ \cdots \\ &+ (2^{\rho-1}-2) \sum_{1\leq i\leq\rho} \phi_h(p_i) \\ &+ (2^\rho-2)\phi_h(1). \end{aligned} \tag{2.7}$$

Beweis: (Bem.: ϕ_h ist multiplikativ, also gilt $\phi_h(1) = 1$.)
Wir gruppieren alle n Signaturen $(\chi_1, \ldots, \chi_\rho)_\nu$ in Abhängigkeit von ν in:

$\binom{\rho}{2}$ Signaturen mit genau zwei $\chi_r = 0$,

$\binom{\rho}{3}$ Signaturen mit genau drei $\chi_r = 0$,

$\ldots$

$\binom{\rho}{\rho}$ Signaturen mit genau ρ $\chi_r = 0$.

Alle diese Gruppierungen sind disjunkt, da trivialerweise für $k \neq l$ gilt

$$(\chi_1, \ldots, \chi_\rho)_k \neq (\chi_1, \ldots, \chi_\rho)_l.$$

Benutzt man noch das Lemma 2.5.2, so folgt die Behauptung.

$\square$

Mit Hilfe der in der Definition 1.1.5.1 auf Seite 25 eingeführten elementarsymmetrischen Funktionen läßt sich für die Summe (2.7) eine überraschend einfache geschlossene Formel finden. Sei weiterhin $n = p_1 \cdots p_\rho$ quadratfrei. Setzen wir

$$\xi_1 = \phi_h(p_1) = p_1 - 2 \quad , \ldots , \quad \xi_\rho = \phi_h(p_\rho) = p_\rho - 2$$

so folgt mit dem in der Definition 1.1.5.1 benutzten Polynom $p(x)$ einerseits, daß $p(2) = n$ ist, andererseits folgt aber wegen

$$\begin{aligned}
\Sigma_1 &= \sum_{r=1}^{\rho} (p_r - 2) \\
\Sigma_2 &= \sum_{1 \leq r < s \leq \rho} (p_r - 2)(p_s - 2) \\
&\vdots \\
\Sigma_\rho &= (p_1 - 2) \cdots (p_\rho - 2),
\end{aligned}$$

daß

$$
\begin{aligned}
\Phi(n) &= 2^\rho + 2^{\rho-1}\Sigma_1 + \cdots + 2^2\Sigma_{\rho-2} \\
&\quad -2 - 2\Sigma_1 - \cdots - 2\Sigma_{\rho-2} \\
&= 2^\rho + 2^{\rho-1}\Sigma_1 + \cdots + 2^2\Sigma_{\rho-2} + 2\Sigma_{\rho-1} + \Sigma_\rho \\
&\quad -2 - 2\Sigma_1 - \cdots - 2\Sigma_{\rho-2} - 2\Sigma_{\rho-1} - \Sigma_\rho \\
&= p(2) - 2\sum_{r=1}^{\rho-1}\Sigma_r - \Sigma_\rho - 2 \\
&= n - 2\sum_{r=1}^{\rho-1}\Sigma_r - \Sigma_\rho - 2, \qquad (2.8)
\end{aligned}
$$

was uns von den lästigen 2er Potenzen befreit. Durch einen weiteren Trick, nämlich mit der Identität für die Eulersche ϕ-Funktion

$$p(1) = \phi(n) = 1^\rho + \sum_{r=1}^{\rho-1}\Sigma_r + \Sigma_\rho$$

gilt

$$-2\phi(n) = -2\sum_{r=1}^{\rho-1}\Sigma_r - \Sigma_\rho - 2 - \Sigma_\rho,$$

so daß mit (2.8) schließlich folgt

$$
\begin{aligned}
\Phi(n) &= n - 2\phi(n) + \Sigma_\rho \\
&= n - 2\phi(n) + \phi_h(n), \quad \forall\, n \in \mathbb{N}, \mu(n) \neq 0. \qquad (2.9)
\end{aligned}
$$

Nun müssen wir die Formel (2.9) noch auf alle $n \in \mathbb{N}$ ausdehnen, und zwar so, daß sie ihrer kombinatorischen Bedeutung, nämlich als Zählfunktion der 00_n-Paare, Rechnung trägt. Ersetzen wir in (2.9) die Funktionen ϕ_h und ϕ durch ihre Produktdarstellungen, so stellen wir fest, daß offenbar

$$\Phi(n) = n - 2n\prod_{\substack{p|n \\ p>3}}\left(1 - \frac{1}{p}\right) + n\prod_{\substack{p|n \\ p>3}}\left(1 - \frac{2}{p}\right) \qquad \forall\, n \in \mathbb{N} \qquad (2.10)$$

gilt. Dabei sind leere Produkte durch 1 zu ersetzen. Für jede Primzahl $p > 3$, $\alpha \geq 0$ gilt ja

$$\Phi(p^\alpha) = p^\alpha - 2(p^\alpha - p^{\alpha-1}) + p^\alpha - 2p^\alpha = 0,$$

da es nicht möglich ist, daß p gleichzeitig $6\nu - 1$ und $6\nu + 1$ teilt für $\nu = 1, \ldots, p^\alpha$. Für $n = 2^\alpha \cdot 3^\beta$ gilt ebenfalls $\Phi(n) = 0$. Ist $n \in \mathbb{N}$ beliebig, so läßt sich stets eine Zerlegung mit $n = d \cdot n'$ finden, wobei n' der größte noch quadratfreie Teiler von n ist mit $\mathrm{ggT}(n', 6) = 1$. Gilt $n' = 1$, so ist $\Phi(n) = 0$, wie gezeigt. Für $n' > 1$ ist aber $n' \in \mathbb{N}_6$ und $\Phi(n')$ nach der Formel (2.9) zu berechnen und mit $d \cdot \Phi(n') = \Phi(n)$ zu multiplizieren. Denn die Folge der Werte der charakteristischen Funktion

$$g_{n'}(\nu) = \begin{cases} 1, & \text{wenn } (6\nu - 1, 6\nu + 1) \text{ ein } 00_{n'}\text{-Paar ist} \\ 0 & \text{sonst.} \end{cases}$$

hat wegen $6(\nu + kn') \pm 1 \equiv \ 6\nu \pm 1 \bmod n'$ die Periode n'. Daraus folgt die Formel (2.10). Φ ist nicht multiplikativ.

$\square$

Bemerkung: Die Gleichung (2.10) kann man auch so ausdrücken:

$$\#00_n\text{-Paare} = n - (\#01_n\text{-Paare} + \#10_n\text{-Paare}) + \#11_n\text{-Paare}.$$

In dieser Form wird die Analogie zur Gleichung (2.2) offensichtlich. Dort stand die Beziehung

$$\#\text{cc-Paare} = n - (\#\text{cp-Paare} + \#\text{pc-Paare}) + \#\text{pp-Paare},$$

genauer die Gleichung

$$B_{cc}(n) = n - \pi(6n + 1) + \pi_2(6n + 1) + 1, \tag{2.11}$$

wobei die 1 am Ende sich einfach daraus ergibt, daß zwei Primzahlen 2 und 3 in $\pi(6n + 1)$ zu viel abgezogen werden und in $\pi(6n + 1)$ ein Zwilling $(3, 5)$ wieder hinzukommt, so daß $-2 + 1 + 1$ die Gleichung wieder herstellt.

Diese Analogie bildet die Grundidee des folgenden Abschnitts. Wir werden dort versuchen, die genaue Formel (2.10) für 00_M-Paare zur Approximation von $B_{cc}(n)$ (also der Anzahl der cc-Paare) unter geeigneter Wahl der Zahlen M und n heranzuziehen.

2.6 $\mathcal{B}_{cc}(n)$ und Φ im Vergleich

Sei $n = p_1 \cdots p_\rho$ das Produkt aufeinaderfolgender Primzahlen $p > 3$, d.h. $p_1 := 5, p_2 := 7, \ldots$. Wir rufen uns die Definition der charakteristischen

Funktion

$$g_n(\nu) = \begin{cases} 1, & \text{wenn } (6\nu-1, 6\nu+1) \text{ ein } 00_n\text{-Paar ist} \\ 0 & \text{sonst} \end{cases}$$

ins Gedächtnis und setzen für alle $x \leq n$

$$G(n,x) : \#\{(6\nu-1, 6\nu+1) \in \mathcal{B}_{cc}(n) : g_n(\nu) = 1, \nu = 1, \ldots, \lfloor x \rfloor\},$$

Die Größe $G(n,x)$ zählt also genau die Paare $(6\nu-1, 6\nu+1)$ für $\nu = 1, \ldots, \lfloor x \rfloor$, wo sowohl $6\nu - 1$ als auch $6\nu + 1$ zusammengesetzte Zahlen sind und wo beide Zahlen mit n mindestens einen gemeinsamen Primteiler haben. Aus den jeweiligen Definitionen folgt nun die Beziehung

$$\Phi(n) \quad = \quad G(n,n) + \mathcal{O}(p_\rho)\,, \tag{2.12}$$

denn für $x = n$ beträgt die Anzahl der Fälle mit $g_n(\nu) = 1$ genau $\Phi(n)$ und die Zusatzbedingung, alle Paare sollen vom cc-Typ sein, ist mit Sicherheit für $\nu = \kappa(p_\rho) + 1, \ldots, n$ erfüllt. Denn die Fälle pp, pc, oder cp können dort nicht mehr eintreten, weil sonst $p > p_\rho$ und p zu n teilerfremd wäre und somit das entsprechende Paar auch kein 00_n-Paar mehr. Für $\nu = 1, \ldots, \kappa(p_\rho)$ können 00_n-Paare wohl die Typen pp, pc oder cp haben, und dies erklärt den Fehlerterm $\mathcal{O}(p_\rho)$.

Wir wollen in $\Phi(n)$ ebenfalls einen weiteren Freiheitsgrad zulassen und definieren für eine noch näher zu spezifizierende Zahl $y \geq p_\rho$

$$\Phi(n,y) := n - 2n \prod_{3<p\leq y}\left(1 - \frac{1}{p}\right) + n \prod_{3<p\leq y}\left(1 - \frac{2}{p}\right).$$

Als nächstes definieren wir τ dadurch, daß p_τ die größte Primzahl $\leq y$ ist. Dann gilt $\tau \geq \rho$ wegen $y \geq p_\rho$, und wir können die beiden Zahlen

$$\begin{aligned} M_y &:= p_1 \cdots p_\tau, \\ d_y &:= p_{\rho+1} \cdots p_\tau = \frac{M_y}{n} \end{aligned}$$

bilden. Für alle $y \geq p_\rho$ gilt dann offensichtlich

$$\Phi(n,y) = n - 2n \prod_{3<p\leq p_\tau}\left(1 - \frac{1}{p}\right) + n \prod_{3<p\leq p_\tau}\left(1 - \frac{2}{p}\right) = \frac{\Phi(M_y)}{d_y}. \tag{2.13}$$

Im Bereich $\nu = 1, \ldots, M_y$ gibt es d_y Abschnitte der Länge n. In jedem dieser Abschnitte erzeugen die Primzahlen $p_1, \ldots, p_\tau$ Paare vom Typ 00_{M_y}. Diese Paare wollen wir in jedem Abschnitt zählen und setzen

$$\begin{aligned}
\Phi_1^*(n,y) &:= \# \, 00_{M_y} - \text{Paare für } \nu = 1, \ldots, n \\
\Phi_2^*(n,y) &:= \# \, 00_{M_y} - \text{Paare für } \nu = n+1, \ldots, 2n \\
&\vdots \\
\Phi_{d_y}^*(n,y) &:= \# \, 00_{M_y} - \text{Paare für } \nu = (d_y - 1)n + 1, \ldots, d_y n.
\end{aligned}$$

Damit gilt für alle $y \geq p_\rho$

$$\sum_{t=1}^{d_y} \Phi_t^*(n,y) = \Phi(M_y) = d_y \Phi(n,y). \tag{2.14}$$

und somit ist für alle $y \geq p_\rho$ der Wert von $\Phi(n,y)$ gleich dem Durchschnitt aller $t = 1, \ldots, d_y$ Werte von $\Phi_t^*(n,y)$.

Aus naheliegenden Gründen interessieren wir uns für den Wert von $\Phi_1^*(n,y)$, wenn wir y wachsen lassen. Denn mit wachsendem y decken wir mit $\Phi_1^*(n,y)$ immer mehr cc-Paare im Bereich $\nu = 1, \ldots, n$ ab, deren Anzahl wir bestimmen wollen. Wir finden für alle $p_\rho \leq y \leq 6n+1$

$$\Phi_1^*(n,y) = G(M_y, n) + \mathcal{O}(y), \tag{2.15}$$

denn aus (2.15) wird (2.12), wenn wir $y = p_\rho$ setzen. Nähert sich hingegen y von unten zunächst $\sqrt{6n+1}$, so erhalten wir die Gleichung

$$\Phi_1^*(n, \sqrt{6n+1}) = \mathcal{B}_{cc}(n) + \mathcal{O}\left(\sqrt{6n+1}\right). \tag{2.16}$$

Das Argument für diese Gleichung ähnelt dem für (2.12): Im Bereich $\nu = \kappa(\sqrt{6n+1}) + 1, \ldots, n$ weisen alle Paare sowohl den 00_{M_y}- wie auch den cc-Typ auf. Für $\nu = 1, \ldots, \kappa(\sqrt{6n+1})$ ist nur der Typ 00_{M_y} sicher, was durch den $\mathcal{O}\,()$-Term ausgeglichen wird. Wir bemerken, daß

$$G(M_y, n) \;\geq\; G(M_{y'}, n) \qquad \forall y \geq y'$$

gilt. $G(M_y, n)$ ist also eine insbesondere auf $y \in [p_\rho, \sqrt{6n+1}]$ mit y monoton wachsende Funktion - je größer wir y wählen, also je mehr aufeinanderfolgende Primteiler wir in M_y zulassen, desto größer wird die Anzahl der im

00_{M_y}-Typ berücksichtigten cc-Paare sein. Für $y = \sqrt{6n+1}$ erreicht sie ein Maximum bei $\mathcal{B}_{cc}(n)$ und bleibt für alle $y \geq \sqrt{6n+1}$ konstant, denn mehr als $\mathcal{B}_{cc}(n)$ Paare vom Typ cc kann es für $\nu = 1, \ldots, n$ trivialerweise nicht geben. Diese Überlegungen fassen wir in

$$\begin{aligned} B_{cc}(n) &\geq G(M_y, n) \qquad y \in [p_\rho, 6n+1] &(2.17)\\ B_{cc}(n) &= G(M_y, n) \qquad y \in [\sqrt{6n+1}, 6n+1] &(2.18)\end{aligned}$$

zusammen. Die Betrachtung des gesamten Bereichs $y \in [p_\rho, 6n+1]$ dient zunächst einmal dem allgemeinen Verständnis, was tatsächlich geschieht. Zwar behält die Gleichung (2.15) auch für $y \in]\sqrt{6n+1}, 6n+1]$ ihre Gültigkeit, doch sie wird spätestens dann trivial, wenn $y \ll n$ wird.

Das weitere Vorgehen liegt nun auf der Hand. Die einzige Möglichkeit, sich dem Wert für $B_{cc}(n)$ von unten zu nähern[17], besteht in der Ungleichung (2.17) durch $G(M_y, n)$. Die letztere Größe wird in der Gleichung (2.15) durch $\Phi_1^*(n, y)$ ausgedrückt. Die Hauptschwierigkeit besteht nun darin, daß wir die einzelnen Werte von $\Phi_t^*(n, y)$ für $t = 1, \ldots, d_y$ nur schwer bestimmen können. Die spezielle Wahl von M_y (siehe Definition der Φ_t^*) als Produkt *aufeinanderfolgender* Primzahlen läßt jedoch hoffen, daß für jeden Wert von t die Anzahl der 00_{M_y}-Paare nicht allzusehr variiert, so daß es plausibel scheint, zur Approximation von $\Phi_t^*(n, y)$ den leicht zu berechnenden Durchschnitt $\Phi(n, y)$ heranzuziehen. Wir setzen dazu

$$\Phi_t^*(n, y) = \Phi(n, y) + F_t(y), \qquad t = 1, \ldots, d_y.$$

Danach gibt speziell der Fehlerterm $F_1(y)$ an, um wieviel $\Phi_1^*(n, y)$ bei der Approximation durch $\Phi(n, y)$ verfehlt wird. Damit folgt aus (2.15)

$$G(M_y, n) = \Phi(n, y) + F_1(y) + \mathcal{O}(y) \tag{2.19}$$

und mit (2.2) und (2.17) schließlich die Beziehung

$$\begin{aligned} \pi_2(6n+1) &\geq \pi(6n+1) - n + \Phi(n, y) + F_1(y) + \mathcal{O}(y)\\ &= \pi(6n+1) - 2n \prod_{3<p\leq y} \left(1 - \frac{1}{p}\right)\\ &\quad + n \prod_{3<p\leq y} \left(1 - \frac{2}{p}\right) + F_1(y) + \mathcal{O}(y). \end{aligned} \tag{2.20}$$

[17]Die Annäherung von unten ist wichtig, man rufe sich etwa die Fußnote auf Seite 68 ins Gedächtnis.

Nach Lemma 1.1.4.3 gibt es eine positive Konstante[18] $C_1 = 1.3995\ldots$ mit

$$2n \prod_{5 \le p \le y} \left(1 - \frac{1}{p}\right) \sim C_1 \frac{n}{logy}.$$

Sei $A > 0$ eine beliebig große fest gewählte Zahl. Aus dem Primzahlsatz folgt, daß es Werte von n gibt, so daß für alle $x \ge n$ gilt

$$|\pi(x) - li\ x| = \mathcal{O}\left(\frac{x}{\log^A x}\right). \tag{2.21}$$

Man kann nun ein y so wählen, daß

$$y = \exp\left(C_1 \frac{n}{li\ n + \mathcal{O}\left(n/\log^A n\right)}\right)$$

wird. Damit folgt

$$\pi_2(6n+1) \ \ge \ n \prod_{3 < p \le e^{D_n}} \left(1 - \frac{2}{p}\right) + F_1(e^{D_n}) + \mathcal{O}\left(e^{D_n}\right). \tag{2.22}$$

mit einem für ein festes aber beliebig groß wählbares $A > 0$ definierten Parameter

$$D_n := C_1 \frac{n}{li\ n + \mathcal{O}\left(n/\log^A n\right)}.$$

Wie man sieht, kann man diese Zahl nur numerisch für ein n bestimmen. Sie kann jedoch nicht allzu groß werden. Tchebycheff konnte schon 1851 zeigen[19], daß für genügend große n die Anzahl der Primzahlen $\pi(6n+1)$ größer ist als $0.92129(6n)/\log(6n)$. Mit unserer Wahl von y folgt somit

$$0.92129 \frac{6n}{\log(6n)} \ < \ C_1 \frac{n}{D_n}$$

$$D_n = \log y \ < \ \frac{C_1 \log(6n)}{6 \cdot 0.92129} = \frac{C_1 \log(6n)}{5.4365637}$$

[18] Im Lemma ergibt sich das für $b = 1, d = 6, y = 5, D = 1$ und aus der numerischen Bestimmung des Grenzwertes von $\sum_{5 \le p \le z} (\log(1 - 1/p) + 1/p) \approx -0.050439\ldots$.

[19] Genauer zeigte er, daß für genügend große x gilt

$$0.92129 \frac{x}{\log x} < \pi(x) < 1.0555 \frac{x}{\log x}.$$

also

$$e^{D_n} = y < (6n)^{C_1/5.4365637} = (6n)^{\delta}, \qquad \text{mit festem } 0 < \delta < 1.$$

Dies zeigt, daß der Fehlerterm $\mathcal{O}\left(e^{D_n}\right)$ gegenüber dem asymptotischen Wert des Hauptterms $n\prod_{3<p\le e^{D_n}}\left(1-\frac{2}{p}\right)$, den wir ebenfalls nach Lemma 1.4.3 erhalten können, nicht ins Gewicht fällt, da der letztere die Größenordnung $\mathcal{O}\left(n/\log^2 n\right)$ hat, wenn man D_n mit der anderen Tchebyscheffschen Konstante nach unten abschätzt (vgl. Fußnote zum Tchebyscheffschen Ergebnis).

Sollte die Primzahlzwillingsvermutung (zumindest) für $d = 2$ richtig sein, eröffnet die Gleichung (2.22) einen neuen Zugang zu ihrer Bestätigung. Man müßte nun überprüfen, ob der Fehlerterm

$$F_1(e^{D_n}) = \Phi_1^*(n, e^{D_n}) - \Phi(n, e^{D_n})$$

klein gegenüber dem Hauptterm ausfällt.

Der Verfasser vermutet, daß es stets Werte von y mit $y \ll n$ gibt, für die $\Phi_t^*(n,y)$ nur "wenig" von ihrem Durchschnittswert $\Phi(n,y)$ abweichen, also für die insbesondere der Fehlerterm $F_1(y)$ klein ist. Die Definition der Φ_t^* auf Seite 78 macht diese Vermutung ebenso plausibel wie numerische Auswertungen, die vom Autor für $F_1(y)$ für verschiedene Kombinationenen von n und y durchgeführt wurden, auf die hier nicht weiter eingegangen werden soll. Leider sieht der Verfasser im jetzigen Stadium keinen Weg für den Beweis dieser Vermutung.

Aber vielleicht gibt es einen anderen Beweisweg: Die Funktion $\Phi_1^*(n,y)$ ist ja gerade so definiert, das sie die Anzahl der Paare $(6k-1, 6k+1)$, $k \le n$ zählt, die $\mathrm{gPf}(6k-1) \le y$ und $\mathrm{gPf}(6k+1) \le y$ erfüllen. Hier fällt die Ähnlichkeit zur Definition der $\Psi(n,y)$-Funktion aus (1.57) auf. Wie man dort sah, gibt es Differenzen-Differentialgleichungen, die für $\Psi(n,y)$ eine asymptotische Formel liefern. Vielleicht gibt es auch solche Gleichungen für $\Phi_t^*(n,y)$. Denn diese Funktionen messen das simultane Aufeinandertreffen der von $\Psi(n,y)$ gezählten Zahlen in den Progressionen $6k-1$ und $6k+1$. Mit solchen Differenzen-Differentialgleichungen ließe sich möglicherweise eine zu (1.57) ähnliche asymtotische Formel finden, von der man nur noch verlangen müßte, daß ihr Fehlerterm die Größenordnung $o\left(n/\log^2 n\right)$ hat und daß sie sich ähnlich einfach wie in (2.20) mit $\pi(6n+1) - n$ "verrechnen" läßt. Damit könnte man auf die Ersetzung von $\Phi_1^*(n,y)$ durch $\Phi(n,y)$, die uns den Fehler $F_1(e^{D_n})$ beschert hat, verzichten und stattdessen diese asymptotische Formel benutzen.

Kapitel 3

Die Anzahl der Primzahlzwillinge zwischen p und p^2.

In diesem Kapitel wird mit Hilfsmitteln der diskreten Fouriertransformation unter anderen eine Formel für die im Titel dieses Kapitels versprochene Größe hergeleitet. Sie besteht im Wesentlichen aus einem Hauptterm der Form $n\prod(1-2/q)$, wobei das Produkt über alle Primzahlen $3 < q \leq p$ läuft und einem komplizierten Restterm, der genau angibt, um wieviel dieses Produkt die tasächliche Anzahl der Primzahlzwillinge zwischen p und p^2 verfehlt. Einige numerische Untersuchungen, die hier ebenfalls vorgestellt werden sollen, zeigen, daß der Restterm meistens negativ zu sein scheint.

3.1 Vorbereitungen und Ideenschilderung

Sei im folgenden $p_\rho > 3$ stets eine Primzahl und

$$N := \prod_{3<p\leq p_\rho} p.$$

Wie im Kapitel 2, wollen wir die Eigenschaften der "siebenden" Funktion

$$s_\rho(k) := \begin{cases} 1, & \text{falls } \operatorname{ggT}(36k^2-1, N) = 1, \\ 0 & \text{sonst} \end{cases} \qquad k = 1, \ldots, N$$

studieren. Wegen $\operatorname{ggT}(36(zN+k)^2-1, N) = \operatorname{ggT}(36k^2-1, N)\ \forall z \in \mathbb{Z}$ läßt sich s_ρ mit Periode N auf ganz $\mathbb{Z}$ periodisch fortsetzen. Von nun an denken wir uns also $s_\rho(k)$ als eine unendliche Folge, die für $k = \ldots, -2, -1, 0, 1, 2, \ldots$ definiert ist.

Unsere Untersuchungen haben zum Ziel, eine möglichst genaue Darstellung für die nicht trivial zu berechnenden Summen

$$S(n) := \sum_{k=0}^{n} s_\rho(k) = \sum_{k=0}^{n} \sum_{d | \operatorname{ggT}(36k^2-1,N)} \mu(d) \tag{3.1}$$

zu finden.

Das Interesse an dieser Summe ist offensichtlich. Mit der aus Kapitel 2 bekannten Abbildung

$$\kappa : \mathbb{R} \to \mathbb{Z}, \qquad \kappa(a) := \left\lfloor \frac{a+1}{6} \right\rfloor \ \forall\, a \in \mathbb{R}.$$

läßt sich nämlich wegen der besonderen Wahl von s_ρ die folgende Beziehung angeben:

$$S(n) = \pi_2(6n+1) - \pi_2(p_\rho) + \theta_\rho \tag{3.2}$$

für alle $n = \kappa(p_\rho) + 1, \ldots, \kappa(p_\rho^2)$, wobei

$$\theta_\rho = \begin{cases} 1, & \text{falls } (p_\rho, p_\rho + 2) \text{ keine Primzahlzwillinge sind,} \\ 0 & \text{sonst} \end{cases}$$

gesetzt wird. Genau an den Stellen nämlich, wo $(6n-1, 6n+1)$ ein Primzahlzwilling mit $p_\rho < 6n-1 < 6n+1 \le p_\rho^2$ ist, wird $\operatorname{ggT}(36n^2-1, N) = 1$, und deshalb erfährt dort die Summe $S(n)$ einen Zuwachs um 1, sonst bleibt der Summenwert konstant[1].

Wegen der Periodizität von s_ρ läßt sich diese Folge mit Hilfe der **diskreten Fouriertransformation (DFT)** anders schreiben. Mit der Fouriertransformierten von s_ρ werden wir eine Formel für $S(N)$ für alle $n = 0, \ldots, N-1$ gewinnen, doch uns interessiert natürlich insbesondere der Bereich $n = \kappa(p_\rho) + 1, \ldots, \kappa(p_\rho^2)$.

[1]Der Grund dafür, daß man zu der Differenz $\pi_2(6n+1) - \pi_2(p_\rho)$ noch $\theta_\rho = 1$ addieren muß, falls $(p_\rho, p_\rho + 2)$ keine Zwillinge sind, ist der, daß $s_\rho(0) = 1$ ist und daß in (3.1) ab $k = 0$ summiert wird. Falls aber $(p_\rho, p_\rho + 2)$ doch Zwillinge sind, geht diese 1 bereits in der Differenz $\pi_2(p_\rho + 2) - \pi_2(p_\rho)$ auf, und deshalb wird für diesen Ausnahmefall $\theta_\rho = 0$ verlangt.

Um später den roten Faden nicht aus den Augen zu verlieren, stellen wir noch einige einfache Rechenhilfen und Ergebnisse zusammen.
Wir nennen von nun an eine beliebige (komplexwertige) Folge $(g)_{k\in\mathbb{Z}}$ mit der Periode $T \in \mathbb{N}$ **gerade**, falls $g(k) = g(-k)\ \forall k \in \mathbb{Z}$ und **ungerade**, falls $g(k) = -g(-k)\ \forall k \in \mathbb{Z}$ ist.

Da wir im folgenden meist im Bereich $k = 0, \ldots, N-1$ rechnen werden, verstehen wir dort unter "negativem" Index einfach $g(-k) := g(N-k)$, falls N die Periode von g ist. Es macht Sinn, statt des Bereichs $k = 1, \ldots, N$ den Bereich $k = 0, \ldots, N-1$ zu benutzen, da im folgenden viele geometrische Summen zu berechnen sein werden.

Wir stellen fest: $s_\rho(k)$ ist eine gerade Folge mit $s_\rho(0) = 1$. Für beliebige $k \in \mathbb{Z}$ gilt nämlich trivialerweise $\mathrm{ggT}(36(N-k)^2-1, N) = \mathrm{ggT}(36k^2-1, N)$ und $\mathrm{ggT}(36(Nk)^2-1, N) = 1$.
Ferner läßt sich jede T-periodische Folge $(g)_k$ wegen

$$g(k) = g^{gerade}(k) + g^{ungerade}(k)$$

in ihren geraden und ungeraden Anteil zerlegen gemäß

$$g^{gerade}(k) = \frac{1}{2}(g(k) + g(-k)), \qquad g^{ungerade}(k) = \frac{1}{2}(g(k) - g(-k)).$$

Trivial ist also, daß für eine gerade Folge wie $s_\rho(k)$ stets $s_\rho k = \frac{1}{2}(s_\rho(k) + s_\rho(-k))$ gilt, was später einfach benutzt wird, ohne daß darauf gesondert eingegangen wird.
Besonders praktisch für die DFT ist die Abkürzung

$$e(\alpha) := \exp(2\pi i\alpha), \qquad \forall\alpha \in \mathbb{R},$$

die von nun an andauernd benutzt wird.

Es gibt viele Möglichkeiten, Formeln für die DFT aufzustellen, wobei alle gleichwertig verwendbar sind. Die Gleichungen (3.3) und (3.4) weiter unten stellen nur eine dieser Möglichkeiten dar. Man findet aber auch Versionen, wo die Vorzeichen in den Exponenten gerade mal vertauscht sind, oder wo der Normierungsfaktor $1/N$ nicht bei den Fourierkoeffizienten, sondern bei der Folge selbst zu finden ist. Alle diese Formeln sind äquivalent, und ihre Wahl hat keine Auswirkung auf das spätere Ergebnis, das hier hergeleitet wird. Zur Theorie der diskreten Fouriertransformation ist das liebevoll geschriebene Buch von Jerri [24] besonders zu empfehlen, das an Detail und Vollständigkeit kaum zu überbieten ist. Eine sehr verständliche Einführung findet man auch in Butz [11].

Die Grundlage für die DFT liefern die Eigenschaften der **N-ten Einheitswurzeln** $e\left(\frac{n}{N}\right)$, die auf ganz $n \in \mathbb{Z}$ eine N-periodische Funktion darstellen. Im Zähler n kommt es also lediglich auf die Restklasse modulo N an. Ferner gilt $e\left(\frac{nN}{N}\right) = 1$ für alle ganzen n. Grundlegend für die DFT ist, daß

$$\sum_{j=0}^{N-1} e\left(\frac{(k-l)j}{N}\right) = \begin{cases} N & \text{für } k \equiv l(N) \\ 0 & \text{sonst.} \end{cases}$$

Die Summe verschwindet nämlich, falls $k \neq l$ ist[2], was etwa aus der geometrischen Summenformel sofort folgt. Für $k = l$ aber wird N-mal die 1 summiert.

Wegen dieser einfachen Eigenschaften lassen sich mit den **diskreten Fourierkoeffizienten**[3]

$$c_\rho(j) := \frac{1}{N} \sum_{k=0}^{N-1} s_\rho(k) e\left(\frac{-kj}{N}\right), \qquad j = 0, \ldots, N-1 \tag{3.3}$$

die so transformierten Werte $s_\rho(k)$ zurückgewinnen gemäß

$$s_\rho(k) = \sum_{j=0}^{N-1} c_\rho(j) e\left(\frac{kj}{N}\right), \qquad k = 0, \ldots, N-1. \tag{3.4}$$

Dies folgt einfach wegen

$$\begin{aligned} s_\rho(k) &= \sum_{j=0}^{N-1} c_\rho(j) e\left(\frac{kj}{N}\right) = \sum_{j=0}^{N-1} \frac{1}{N} \sum_{l=0}^{N-1} s_\rho(l) e\left(\frac{-lj}{N}\right) e\left(\frac{kj}{N}\right) \\ &= \frac{1}{N} \sum_{l=0}^{N-1} s_\rho(l) \sum_{j=0}^{N-1} e\left(\frac{(k-l)j}{N}\right) = \frac{1}{N} s_\rho(k) N \end{aligned}$$

für $k = 0, \ldots, N-1$.

[2]Mit Periode N fortgesetzt bedeutet dies $k \not\equiv l(N)$.

[3]Man beachte, daß an die komplexwertige Folge $s_\rho(k)$, $k = 0, \ldots, N-1$ keine zusätzlichen Bedingungen gestellt werden, außer vielleicht, daß alle $s_\rho(k)$ endlich sein müssen. Insofern gelten die hier vorgestellten Gleichungen nicht nur für unsere spezielle Folge s_ρ, sondern ganz allgemein.

Es ist außerdem klar, daß sich die Folge der Fourierkoeffizienten $c_\rho(j)$, $j = 0, \ldots, N-1$ mit der Periode N auf ganz $j \in \mathbb{Z}$ periodisch fortsetzen läßt. Von nun an seien also auch die $c_\rho(j)$ für alle $j \in \mathbb{Z}$ definiert.

Für spätere Untersuchungen brauchen wir noch die folgenden Ergebnisse:

Lemma 3.1.1 *Die diskreten Fourierkoeffizienten einer jeden geraden reellwertigen Folge sind reell.*

Beweis: O.B.d.A. rechnen wir das am Beispiel von $s_\rho(k)$ nach.
Es gilt für $j = 0, \ldots, N-1$:

$$\begin{aligned}
c_\rho(j) &= \frac{1}{N}\sum_{k=0}^{N-1}\frac{1}{2}(s_\rho(k)+s_\rho(-k))e\left(\frac{-kj}{N}\right) && \text{(weil } s_\rho \text{ gerade)}\\
&= \frac{1}{2}\left\{\frac{1}{N}\sum_{k=0}^{N-1}s_\rho(k)e\left(\frac{-kj}{N}\right)+\frac{1}{N}\overline{\sum_{k=0}^{N-1}s_\rho(k)e\left(\frac{-kj}{N}\right)}\right\} && (s_\rho \text{ reell})\\
&= \frac{1}{2}\left(c_\rho(j)+\overline{c_\rho(j)}\right) = \Re(c_\rho(j)).
\end{aligned}$$

□

Lemma 3.1.2 *Ist $(s_\rho)_k$ eine reelle gerade Folge, dann ist die Folge ihrer diskreten Fourierkoeffizienten $(c_\rho)_j$ auch gerade.*

Beweis: Es gilt für $j = 0, \ldots, N-1$:

$$\begin{aligned}
c_\rho(j) &= \frac{1}{N}\sum_{k=0}^{N-1}s_\rho(k)e\left(\frac{-kj}{N}\right)\\
&= \frac{1}{N}\overline{\sum_{k=0}^{N-1}s_\rho(k)e\left(\frac{-kj}{N}\right)} && (c_\rho \text{ reell})\\
&= \frac{1}{N}\sum_{k=0}^{N-1}s_\rho(k)e\left(\frac{kj}{N}\right) && (s_\rho \text{ reell})\\
&= \frac{1}{N}\sum_{k=0}^{N-1}s_\rho(k)e\left(\frac{-k(-j)}{N}\right) = c_\rho(-j).
\end{aligned}$$

□

Lemma 3.1.3 *Für jede N-periodische Folge $(s_\rho)_k$ gilt $\sum_{j=0}^{N-1} c_\rho(j) = s_\rho(0)$, falls c_ρ ihre diskreten Fourierkoeffizienten sind.*

Beweis:

$$\begin{aligned}\sum_{j=0}^{N-1} c_\rho(j) &= \sum_{j=0}^{N-1} \frac{1}{N} \sum_{k=0}^{N-1} s_\rho(k) e\left(\frac{-kj}{N}\right)\\ &= \sum_{k=0}^{N-1} \frac{1}{N} s_\rho(k) \sum_{j=0}^{N-1} e\left(\frac{-jk}{N}\right)\\ &= \frac{1}{N} \sum_{k=0}^{N-1} s_\rho(k)(k=0) = \frac{1}{N} s_\rho(0) N.\end{aligned}$$

□

Obwohl dieses Lemma ganz allgemein gilt, folgt mit unserer Folge $(s_\rho)_k$ also

$$\sum_{j=0}^{N-1} c_\rho(j) = s_\rho(0) = 1. \tag{3.5}$$

Weiter stellen wir fest:

$$c_\rho(0) = \frac{1}{N} \sum_{k=0}^{N-1} s_\rho(k) = \frac{S(N-1)}{N}. \tag{3.6}$$

Dieses besondere Verhältnis wird für uns eine wichtige Rolle spielen. Summiert man nämlich in (3.1) bis $n = N-1$, so wird

$$\begin{aligned}S(N-1) &= \sum_{k=0}^{N-1} \sum_{d \mid \mathrm{ggT}(36k^2-1, N)} \mu(d) = \sum_{d \mid N} \mu(d) \sum_{\substack{0 \le k \le N-1 \\ 36k^2 \equiv 1(d)}} 1\\ &= \sum_{d \mid N} \mu(d) \frac{N}{d} 2^{\omega(d)} = N \prod_{p \mid N} \left(1 - \frac{2}{p}\right) = N \prod_{3 < p \le p_\rho} \left(1 - \frac{2}{p}\right).\end{aligned}$$

Die Summen $S(n)$, $n = 0, \ldots, N-1$ sind also alle ≥ 1 und bilden für $n \in [0, N[$ eine monoton steigende Treppenfunktion, an deren Sprungstellen wir interessiert sind und die für $n = N-1$ den Wert $\phi_h(N)$ annimmt, wobei die multiplikative Funktion ϕ_h schon im Kapitel 2 benutzt wurde.

Zieht man nun durch die Punkte $(0,0)$ und $(N-1, S(N-1))$ eine Gerade, so hat diese nach Lemma 1.1.4.3 die asymtotische Steigung

$$\tan(\gamma) := \frac{S(N-1)}{N} = \prod_{3 < p \le p_\rho} \left(1 - \frac{2}{p}\right) \sim C \frac{1}{\log^2(p_\rho)},$$

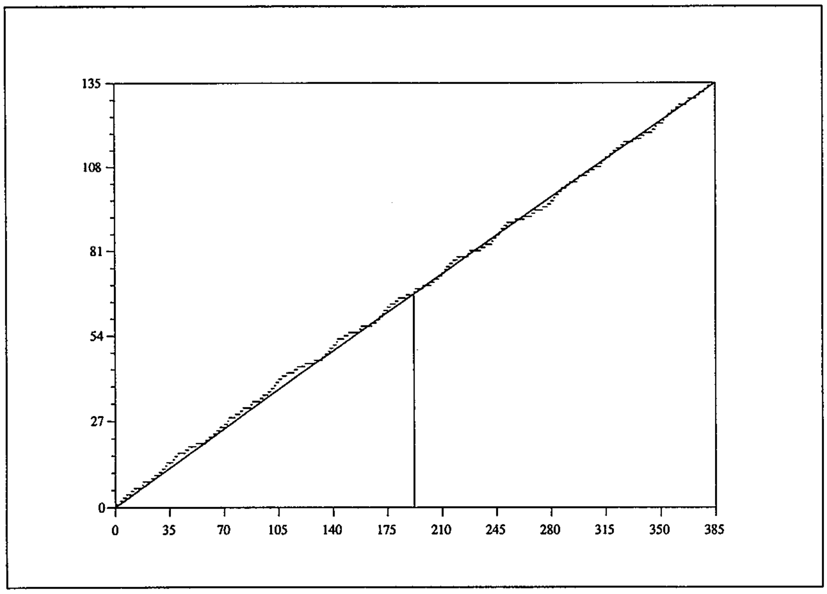

Abbildung 3.1: $S(n)$ für $n = 0, \ldots, N-1$ für $N = 5 \cdot 7 \cdot 11$ (Treppenfunktion) und die zugehörige Steigungsgerade.

wobei die Konstante C von p_ρ und somit von N unabhängig ist.
In der Abbildung 3.1 sieht man den Fall für $N = 385 = 5 \cdot 7 \cdot 11$. Obwohl man es an der Zeichnung nicht erkennen, bleibt $S(n)$ für $n = 0, 1, 2$ zuerst konstant auf 1, da $(6 \cdot 1 - 1, 6 \cdot 1 + 1) = (5, 7)$ und $(6 \cdot 2 - 1, 6 \cdot 2 + 1) = (11, 13)$ zunächst einmal Zwillinge sind, die Primzahlen enthalten, die auch N teilen. Wegen $\kappa(11) = 2$ und $\kappa(11^2) = 20$ interessieren wir uns für den Bereich $n = 3, \ldots, 20$. An den Stellen $3, 5, 7, 10, 12, 17, 18$ erhöht sich $S(n)$ schließlich auf den Wert 8, was die 7 Zwillinge $(17, 19)$, $(29, 31)$, $(41, 43)$, $(59, 61)$, $(71, 73)$, $(101, 103)$ und $(107, 109)$ zählt. Danach steigt $S(n)$ sprunghaft weiter, wir können aber nicht mehr von Primzahlzwillingen sprechen, sondern höchstens von Zahlenpaaren $(6n - 1, 6n + 1)$, in denen weder $6n - 1$ noch $6n + 1$ durch eine der Primzahlen $5, 7, 11$ teilbar ist.

Nun könnte man erwarten, daß der Wert $S(n)$ nur "wenig" vom Wert

$$f(n) := n \tan(\gamma)$$

abweicht, die Differenz $S(n) - f(n)$ also vernachlässigbar gegenüber dem asymtotischen "Mittelwert" $Cn/\log^2(p_\rho)$ ist, wenn wir p_ρ gegen Unendlich gehen lassen und $S(n)$ und $f(n)$ für jeweils die neuen Werte N und γ berechnen. Zum Beispiel muß es irgendwo in der Nähe des Punktes[4]

$$\delta := \frac{N-1}{2}$$

einen Wert geben, den die beiden Funktionen annehmen (d.h. die Gerade $f(n)$ "schneidet" die Treppenfunktion $S(n)$), weil die Folge $(s_\rho)_k$ gerade ist.

Andererseits gibt es aber ganze Bereiche, die doppelt vorhanden sind und symmetrisch zu δ liegen, wo die Funktion $S(n)$ konstant bleibt. Beispielsweise sind es sicher die Bereiche $n = 0, \ldots, \kappa(p_\rho)$ mit $S(n) = 1$ (aus oben erwähnten Gründen) und $n = N - \kappa(p_\rho) - 1, \ldots, N-1$ (aus Symmetriegründen), wo $S(n)$ bereits ihren Höchstwert $S(N-1)$ erreicht hat.

Uns interessiert natürlich in besonderem Maße das Verhalten von $S(n)$ im Bereich $n = \kappa(p_\rho) + 1, \ldots, \kappa(p_\rho^2)$, an dessen Ende die Gerade den asymptotischen Wert

$$f(\kappa(p_\rho^2)) \sim \kappa(p_\rho^2) \cdot C\frac{1}{\log^2 p_\rho} = 4C\frac{\frac{p_\rho^2-1}{6}}{\log^2 p_\rho^2} = \frac{2}{3}C\frac{p_\rho^2}{\log^2 p_\rho^2} \tag{3.7}$$

annimmt[5].

Diese Betrachtungen sind zwar für den aufmerksamen Leser offensichtlich und deshalb vielleicht uninteressant. Man sollte sie aber stets im Hinterkopf behalten, denn sie bilden die Seele der folgenden trockenen mathematischen Überlegungen.

Aus (3.5) und (3.6) folgt noch

$$\sum_{j=1}^{N-1} c_\rho(j) = 1 - \tan(\gamma) \qquad \text{und} \qquad \sum_{j=1}^{\delta} c_\rho(j) = \frac{1}{2}(1 - \tan(\gamma)), \tag{3.8}$$

weil c_ρ gerade ist. Die $c_\rho(j)$, $j = 0, \ldots, N-1$ sind in Wahrheit reellwertig, wie wir gesehen haben. Genauer gilt

$$c_\rho \;=\; \frac{1}{N}\sum_{k=0}^{N-1} s_\rho(k) e\left(\frac{-kj}{N}\right)$$

[4] N ist ungerade, also δ eine ganze Zahl.

[5] Wegen $p^2 \equiv 1(6)$ für alle $p > 3$ ist stets $\kappa(p^2) = \frac{p^2-1}{6}$

$$= \frac{1}{N}\left\{1+\sum_{k=1}^{\delta} s_\rho(k)\underbrace{\left(e\left(\frac{-kj}{N}\right)+e\left(\frac{+kj}{N}\right)\right)}_{=2\Re\left(e\left(\frac{kj}{N}\right)\right)}\right\}$$

$$= \frac{1}{N}+\frac{2}{N}\sum_{k=1}^{\delta} s_\rho(k)\cos\left(\frac{2\pi kj}{N}\right). \tag{3.9}$$

Schließlich brauchen wir noch die folgende Identität, deren Beweis sehr einfach[6] aber langwierig ist, und deshalb hier weggelassen wird:

Lemma 3.1.4 *Sei* $0 \le n \le N-2$ *und* $j \not\equiv 0(N)$. *Dann gilt*

$$\sum_{k=0}^{n} e\left(\frac{jk}{N}\right) = \frac{1}{2}\left(1+e\left(\frac{nj}{N}\right)\right)+\frac{i}{2}\operatorname{ctg}\left(\frac{\pi j}{N}\right)\left(1-e\left(\frac{nj}{N}\right)\right).$$

3.2 Auswertung von $S(n)$ mittels diskreter Fouriertransformation

Nach allen diesen Vorbereitungen können wir endlich mit der Auswertung von $S(n)$ beginnen. Für $0 \le n \le N-2$ gilt

$$\begin{aligned} S(n) &= \sum_{k=0}^{n} s_\rho(k) = \sum_{k=0}^{n}\sum_{j=0}^{N-1} c_\rho(j) e\left(\frac{jk}{N}\right) \\ &= \sum_{j=0}^{N-1} c_\rho(j)\sum_{k=0}^{n} e\left(\frac{jk}{N}\right) \\ &= \underbrace{c_\rho(0)(n+1)}_{(3.6)} + \sum_{j=1}^{N-1} c_\rho(j)\underbrace{\sum_{k=0}^{n} e\left(\frac{jk}{N}\right)}_{Lemma\ 3.1.4} \\ &= \tan(\gamma)(n+1) + \sum_{j=1}^{N-1} c_\rho(j)\left\{\frac{1}{2}\left(1+e\left(\frac{nj}{N}\right)\right)+\right. \end{aligned}$$

[6] Man benutzt die geometrische Summenformel und einige Identitäten mit trigonometrischen Funktionen.

$$
\begin{aligned}
& +\frac{i}{2}\operatorname{ctg}\left(\frac{\pi j}{N}\right)\left(1-e\left(\frac{nj}{N}\right)\right)\Bigg\} \\
= \quad & \tan(\gamma)(n+1) + \underbrace{\frac{1}{2}\sum_{j=1}^{N-1} c_\rho(j)}_{(3.8)\Rightarrow(1-\tan\gamma)/2} + \underbrace{\frac{1}{2}\sum_{j=1}^{N-1} c_\rho(j) e\left(\frac{nj}{N}\right)}_{=(s_\rho(n)-c_\rho(0))/2} \\
& +\frac{i}{2}\sum_{j=1}^{N-1} c_\rho(j)\operatorname{ctg}\left(\frac{\pi j}{N}\right) - \frac{i}{2}\sum_{j=1}^{N-1} c_\rho(j)\operatorname{ctg}\left(\frac{\pi j}{N}\right) e\left(\frac{nj}{N}\right) \\
= \quad & n\tan(\gamma) + \frac{1}{2}(1+s_\rho(n)) - \frac{i}{2}\sum_{j=1}^{N-1} c_\rho(j)\operatorname{ctg}\left(\frac{\pi j}{N}\right) e\left(\frac{nj}{N}\right),
\end{aligned}
$$

weil die Summe

$$
\frac{i}{2}\sum_{j=1}^{N-1} c_\rho(j)\operatorname{ctg}\left(\frac{\pi j}{N}\right)
$$

verschwindet wegen $c_\rho(j) = c_\rho(-j)$ und $\operatorname{ctg}\left(\frac{\pi j}{N}\right) = -\operatorname{ctg}\left(\frac{-\pi j}{N}\right)$. Aus demselben Grund finden wir weiter

$$
\begin{aligned}
& -\frac{i}{2}\sum_{j=1}^{N-1} c_\rho(j)\operatorname{ctg}\left(\frac{\pi j}{N}\right) e\left(\frac{nj}{N}\right) = \\
& -\frac{i}{2}\sum_{j=1}^{\delta} c_\rho(j)\operatorname{ctg}\left(\frac{\pi j}{N}\right)\underbrace{\left(e\left(\frac{nj}{N}\right) - e\left(\frac{-nj}{N}\right)\right)}_{=2i\Im\left(e\left(\frac{nj}{N}\right)\right)} = \\
& +\sum_{j=1}^{\delta} c_\rho(j)\operatorname{ctg}\left(\frac{\pi j}{N}\right)\sin\left(\frac{2\pi nj}{N}\right),
\end{aligned}
$$

so daß schließlich, wie erwartet, eine reellwertige Summe

$$
S(n) = n\tan(\gamma) + \frac{1}{2}(1+s_\rho(n)) + \Sigma_\rho^*(n) \tag{3.10}
$$

herauskommt mit

$$
\Sigma_\rho^*(n) := \sum_{j=1}^{\delta} c_\rho(j)\operatorname{ctg}\left(\frac{\pi j}{N}\right)\sin\left(\frac{2\pi nj}{N}\right). \tag{3.11}
$$

Wir erhalten also für $S(n)$ tatsächlich den erwarteten "Mittelwert" $n\tan(\gamma)$ plus Restglieder. Die Größe $\frac{1}{2}(1+s_\rho(n))$ ist entweder gleich $\frac{1}{2}$ oder 1, je

nachdem, ob $\mathrm{ggT}(36n^2 - 1, N) > 1$ oder $\mathrm{ggT}(36n^2 - 1, N) = 1$ ist. Für $n = \kappa(p_\rho^2)$ steht hier $\frac{1}{2}$, da das Paar $(p_\rho^2 - 2, p_\rho^2)$ sowieso kein Zwilling sein kann.
Da die linke Seite der Gleichung (3.10) stets eine natürliche Zahl ist, muß es auch die rechte sein, obwohl man es nicht ohne Weiteres sehen kann.

Leider führt der Versuch, das Restglied Σ_ρ^* mittels (3.9) nach oben abzuschätzen durch Standardverfahren wie etwa die Cauchy-Schwarzsche Ungleichung, mit und ohne vorherige partielle Summation, nicht zum Erfolg. Die komplexen, unüberschaubaren Vorzeichenwechsel aller drei Faktoren c_ρ, ctg und sin gehen bei solchen Abschätzungen "im Betrag" verloren. Daß durch diese Vorzeichenwechsel sich in der Summe Σ_ρ^* vermutlich dennoch sehr viel Substanz weghebt, zeigt die numerische Auswertung im nächsten Abschnitt.

3.3 Visualisierung des Restglieds Σ_ρ^*

In diesem Abschnitt wird der Restterm Σ_ρ^* zum besseren Verständnis an den Stellen $\kappa(p_\rho^2)$ visualisiert. Zunächst einmal folgt wegen (3.2) und (3.10) insbesondere die Gleichung

$$\pi_2(p_\rho^2) - \pi_2(p_\rho) + \theta_\rho - \kappa(p_\rho^2)\tan(\gamma) - \frac{1}{2} = \Sigma_\rho^*(\kappa(p_\rho^2)). \tag{3.12}$$

Man kann nun Σ_ρ^* auf dreierlei Weise numerisch bestimmen:

1. Man berechnet für ein N die gesamte Folge $s_\rho(k)$, $k = 0, \ldots, N-1$, führt die DFT für $c_\rho(j)$ durch für $j = 0, \ldots, N-1$ und benutzt die Formel (3.11) (die schlechteste Möglichkeit, trotz des FFT-Algorithmus[7]).

2. Man berechnet $s_\rho(k)$, $k = 0, \ldots, N-1$ wie in 1, weiter die Teilsummen $S(n)$, und benutzt die Formel

$$\Sigma_\rho^*(n) = S(n) - n\tan(\gamma) - \frac{1}{2}(1 + s_\rho(n))$$

(eine bessere Wahl).

[7] Die normale diskrete Fouriertransformation benötigt N^2 Rechenoperationen, beim sog. Fast-Fourier-Transform-Algorithmus sind nur $N \log_2 N$ Operationen nötig, vgl. etwa Butz [11].

3. Man berechnet $s_\rho(k)$, $k = 0, \ldots, N-1$ wie oben, und rechnet $\Sigma_\rho^*(n)$ rekursiv aus. Es gilt nämlich wegen

$$\Sigma_\rho^*(n+1) - \Sigma_\rho^*(n) = -\tan(\gamma) + \frac{1}{2}(s_\rho(n) + s_\rho(n+1))$$

$$\Sigma_\rho^*(n+1) = \Sigma_\rho^*(n) - \tan(\gamma) + \frac{1}{2}(s_\rho(n) + s_\rho(n+1)) \tag{3.13}$$

mit $\Sigma_\rho^*(0) := 0$, was ebenfalls sofort aus der Definition (3.11) folgt.

Bemerkung 1) Da wir hauptsächlich an $n = \kappa(p_\rho^2)$ interessiert sind, reicht es in den Fällen 2. und 3. aus, die Folge $s_\rho(k)$ lediglich für $k = 0, \ldots, \kappa(p_\rho^2)$ zu berechnen. Wegen $s_\rho(0) = 1$ und $s_\rho(k) = 0$ für $k = 1, \ldots, \kappa(p_\rho)$ gilt übrigens nach (3.13)

$$\Sigma_\rho^*(n) = -n\tan(\gamma) + \frac{1}{2}, \qquad n = 1, \ldots, \kappa(p_\rho),$$

was praktisch ist, wenn man $\Sigma_\rho^*(n)$ für mehr Werte von n braucht.

Bemerkung 2) Es ist trügerisch, zu hoffen, man könnte die rekursive Formel (3.13) irgendwie "auflösen", da das Verhalten von $s_\rho(n)$, das wir ja gerade herausfinden wollen, für die rekursiven Werte von $\Sigma_\rho^*(n)$ entscheidend ist.

Dennoch fällt hier eine seltsame Parallele zur Welt der Physik ins Auge. In der Nachrichtentechnik werden oft spezielle digitale Filter eingesetzt, um Rückkopplungseffekte bei Life-Sendungen mit Zuschauertelefon auszugleichen. Eine Gleichung der Form (3.13) erinnert stark an ein solches rekursives digitales Filter mit 100% Rückkopplung (Faktor 1 vor $\Sigma_\rho^*(n)$) zwischen dem aufgenommenen "Inputsignal" $s_\rho(n)$, $n = 0, \ldots, N-1$ und dem "Outputsignal" $\Sigma_\rho^*(n)$ (zu Gleichungen diesen Typs siehe Butz [11]). Genauer gesagt würde es sich bei (3.13) um ein Tiefpaßfilter handeln wegen der glättenden Wirkung (Butz) des digitalen Operators

$$\text{output}(n) = \frac{1}{2}(\text{input}(n) + \text{input}(n+1)).$$

Ohne die Konstante $-\tan(\gamma)$ könnte man die Gleichung (3.13) auch als "Trapezregel" für das Integrieren diskreter Daten auffassen:

$$y_{k+1} := y_k + \frac{\Delta t}{2}(f_k + f_{k+1}),$$

wobei f_k, $k = 0, \ldots, N-1$ die in Zeitabständen Δt gesampelte Folge ist und y_k das "Integral" sein soll (Butz). Überraschend ist, daß dann unsere Trapezregel mit $f_k := s_\rho(k)$ nichts anderes als die Summe $S(n)$ liefern würde[8], und nicht den Restterm $\Sigma_\rho^*(n)$, der noch die Konstante $-\tan(\gamma)$ zu seiner Berechnung benötigt.
Zwar folgt daraus mit (3.2), daß $\Sigma_\rho^*(\kappa(p_\rho^2)) < \pi_2(p_\rho^2) - \pi_2(p_\rho) + \theta_\rho$, aber wegen (3.12) könnte es auch sein, daß $\Sigma_\rho^*(\kappa(p_\rho^2)$ auch mal negativ und somit diese "untere Schranke" trivial wird. Damit lautet die viel interessantere Frage also, ob

$$\Sigma_\rho^*(\kappa(p_\rho^2)) > -\kappa(p_\rho^2)\tan(\gamma) - \frac{1}{2} + \theta_\rho \tag{3.14}$$

ist für alle Primzahlen $p_\rho > 3$ und die zugehörigen Werte von γ. Würde hier nämlich fast immer echte Ungleichheit herrschen, dann wäre die Differenz $\pi_2(p_\rho^2) - \pi_2(p_\rho)$ stets positiv und die Folge der Primzahlzwillinge unendlich. Umgekehrt aber, die Endlichkeit der Primzahlzwillinge vorausgesetzt, müßte nach Bemerkung 1)

$$\Sigma_\rho^*(\kappa(p^2)) = -\kappa(p^2)\tan(\gamma) + \frac{1}{2} \tag{3.15}$$

sein *für alle* Primzahlen $p > p_\tau$, falls $(p_\tau, p_\tau + 2)$ der letzte existierende Zwilling ist.

Doch nun zur eigentlichen numerischen Auswertung. Die vom Verfasser erzeugten Daten umfassen die Werte für die ersten 3400 Primzahlen $p_1 = 5, \ldots, p_{3400} = 31627$, also mit $p_{3399}^2 \le 10^9 < p_{3400}^2$, deren Berechnung auf einem Pentium 200MHz etwa 23 Stunden gebraucht hat. Am wenigsten rechenaufwendig schien hier die zweite Möglichkeit von den drei oben genannten Möglichkeiten zu sein, obwohl die dritte besser ist, falls man $\Sigma_\rho^*(n)$ für ein festes ρ für mehr Werte von n studieren will.

Zur Visualisierung wurden in der Abbildung 3.2 die folgenden drei Größen zusammengestellt:

- $\kappa(p_\rho^2)\tan(\gamma) + 1/2$, also der Hauptterm nach (3.10) mit $n = \kappa(p_\rho^2)$.
- der zugehörige Restterm $\Sigma_\rho^*(\kappa(p_\rho^2))$.

[8] vielleicht stellenweise bis auf den Fehler 0.5

- $\pi_2(p_\rho^2) - \pi_2(p_\rho)$. Diese Differenz ergibt sich aus der Summe des Haupt- und Restterms, bis auf den stellenweisen Fehler $\theta = 1$, der hier nicht ins Gewicht fällt,

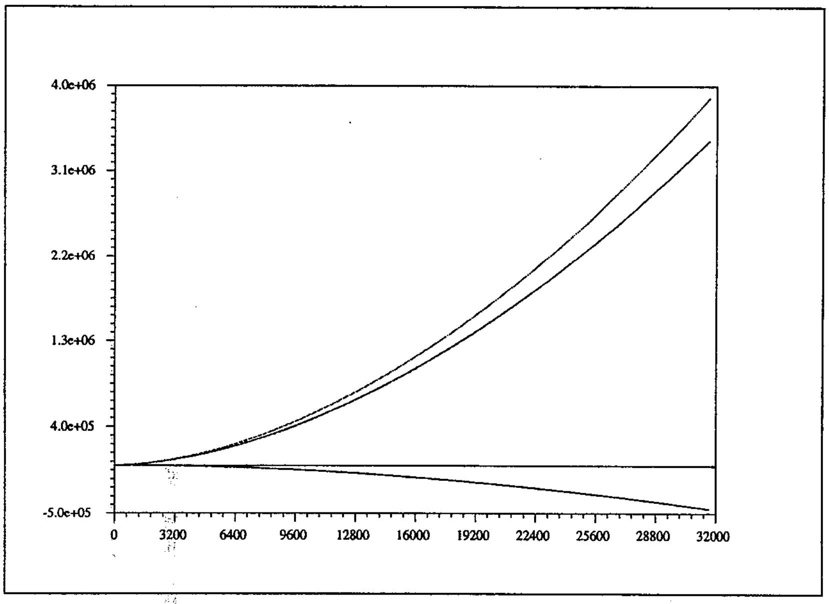

Abbildung 3.2: Der Hauptterm $\kappa(p_\rho^2)\tan(\gamma) + 1/2$, der negative Restterm $\Sigma_\rho^*(\kappa(p_\rho^2))$ und die sich aus ihrer Summe ergebende Differenz $\pi_2(p_\rho^2) - \pi_2(p_\rho)$ (mittlere Linie) für Primzahlen $p^2 \leq 10^9$.

Natürlich wurde für jedes $p_\rho > 3$ der Wert

$$\tan(\gamma) = \prod_{3<p\leq p_\rho} \left(1 - \frac{2}{p}\right)$$

neu berechnet. Die Berechnung eines solchen Produkts ist mit reellwertigen Variablen für derart viele Primzahlen numerisch ungenau, deshalb wurde hier mit rationalen Zahlen beliebiger Genauigkeit mit dem für Zahlentheoretiker empfehlenswerten, konstenlos aus dem Internet downloadbaren Programmpaket PARI 2.0.15 gearbeitet (vgl. Batut u.a. [3]).

Zu Vergleichszwecken wurde auch der Anfang der Wertetabelle 3.1 angefügt. Es fällt auf, daß zumindest im erfaßten Zahlenbereich bis $p_\rho^2 \leq 10^9$

die Anzahl der "neuen" Primzahlzwillinge für wachsendes ρ in den Intervallen $]p_\rho, p_\rho^2]$ mehr als linear wächst, obwohl sich diese Intervalle auch teilweise überlappen. Außerdem sieht man, daß unser Hauptterm größer ist als diese Anzahl, was äquivalent damit ist, daß $\Sigma_\rho^*(\kappa(p_\rho^2))$ negativ wird, obwohl es nicht immer der Fall ist, wie man in der Tabelle sehen kann.

p	$\kappa(p_\rho^2)\tan(\gamma)+1/2$	$\Sigma_\rho^*(\kappa(p^2))$	$S(\kappa(p^2))$	$\pi_2(p)$	$\pi_2(p^2)-\pi_2(p)$
5	2.90000000	0.0999999999	3	1	3
7	3.92857142	1.07142857	5	2	4
11	7.51298701	0.487012987	8	2	8
13	8.80769230	1.19230769	10	3	9
17	13.0662572	2.93374272	16	3	16
19	14.5543666	3.44563331	18	4	17
23	19.3206301	2.67936982	22	4	21
29	28.3769522	0.623047787	29	4	29
31	30.3039304	0.696069524	31	5	30
37	40.6748927	1.32510723	42	5	41
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Tabelle 3.1: Anfang der Wertetabelle, die der Abbildung 3.2 zugrundeliegt. Zunächst ist $\Sigma_\rho^* > 0$.

Die Abbildung 3.4 zeigt $\Sigma_\rho^*(\kappa(p_\rho^2))$ im Detail für die ersten 160 Primzahlen in $]3, 953]$. Daß $\Sigma_\rho^*(\kappa(p^2))$ nicht immer nur negativ ausfällt, bestätigt das Verhalten der Funktion bis zur Primzahl $p = 211$, wo sie hauptsächlich im positiven Bereich oszilliert. Danach bleibt sie durchgehend, zumindest in dem vom Verfasser erfaßten Intervall $211 < p_\rho \leq 10^{9/2}$, im negativen Bereich.

Falls also

$$|\Sigma_\rho^*(\kappa(p_\rho^2))| \leq C_3\kappa(p_\rho^2) \prod_{3<p\leq p_\rho} (1-\frac{2}{p})$$

ist mit einer positiven Konstanten $C_3 < 1$ für $p_\rho \to \infty$, dann gibt es unendlich viele 2-Zwillinge. Die Tabelle 3.2 zeigt, daß es möglicherweise eine solche Konstante gibt, obwohl die Werte des Verhältnisses $C_3(p) := \left|\Sigma_\rho^*(\kappa(p^2))/(\kappa(p^2)\tan(\gamma)+1/2)\right|$ zunächst auf über 11% des Hauptwertes anwachsen.

Gäbe es nur endlich viele Primzahlzwillinge, würde aus der Gleichung (3.15) folgen, daß $\Sigma_\rho^*(\kappa(p_\rho^2))$ bis $\rho \leq \tau$ eine "Zitterfunktion" ist, während sie für alle

n	p mit $p^2 \leq 10^n$	$\kappa(p^2)\tan(\gamma)+1/2$	$\Sigma_\rho^*(\kappa(p^2))$	$C_3(p)$
2	7	3.92857142	1.071428578	0.27272727
3	31	30.3039304	0.696069524	0.02296961
4	97	180.649281	7.35071864	0.04069055
5	313	1206.07455	-22.0745570	0.01830281
6	997	8604.94678	-516.946786	0.06007554
7	3137	62945.4144	-4815.41440	0.07650143
8	9973	486802.694	-48814.6939	0.10027614
9	31607	3870035.41	-449068.414	0.11603729

Tabelle 3.2: Nochmals zur Hardy-Littlewoodschen Vermutung. Diesmal wurde das (vorzeichenlose) Verhältnis von Σ_ρ^* zum Hauptterm gemessen ($C_3(p)$).

Werte $\rho > \tau$ monoton fallen würde. Wir werden anhand der Formel (3.18) des nächsten Abschnitts sehen, daß die natürlichen Zahlen sehr sonderbar beschaffen sein müßten, wenn diese "Beruhigung" von Σ_ρ^* tatsächlich irgendwann einsetzen sollte.

Bevor wir mit der letzten Umformung von Σ_ρ^* beginnen, möchte ich auf noch eine Kuriosität hinweisen. In der Abbildung 3.4 auf Seite 99 sieht man Aufwärtszacken immer dann, wenn $(p_\rho - 2, p_\rho)$ ein Zwilling ist. Mit

$$\Delta_\rho := \Sigma_\rho^*(\kappa(p_\rho^2)) - \Sigma_{\rho-1}^*(\kappa(p_{\rho-1}^2))$$

würde dies, vielleicht bis auf wenige (endlich viele?) Ausnahmen die Ungleichung

$$(p_{\rho-1}, p_\rho) \text{ sind Zwillinge.} \overset{?}{\Rightarrow} \Delta_\rho \geq 0. \tag{3.16}$$

bedeuten. Diese Vermutung wurde vom Verfasser bis $p_\rho^2 \leq 10^9$ getestet. Bis auf die zwei Ausnahmen (71,73), und (461,463) mit den Werten -0.0705784 und -0.0255407 respekive, stimmt diese Vermutung für die restlichen 484 Zwillinge in diesem Bereich. Die Abbildung 3.5 zeigt, daß der Wert von Δ_ρ für Primzahlzwillinge $(p_\rho - 2, p_\rho)$ eher wachsend ist, so daß die Vermutung (3.16) vielleicht tatsächlich richtig ist.

Wachsendes Δ_ρ ist umso erstaunlicher, als daß diese Vorwärtsdifferenz eher negativ ausfällt, und zwar besonders dann, wenn der Abstand zwischen $p_{\rho-1}$ und p_ρ größer wird. So gesehen scheint Σ_ρ^* ein guter Indikator dafür zu sein, wie dicht die Primzahlen $p_{\rho-1}$ und p_ρ beieinander liegen, obwohl eigentlich jedesmal geprüft wird, wie viele Primzahlzwillinge in den Bereichen $]p_{\rho-1}, p_{\rho-1}^2]$ und $]p_\rho, p_\rho^2]$ existieren.

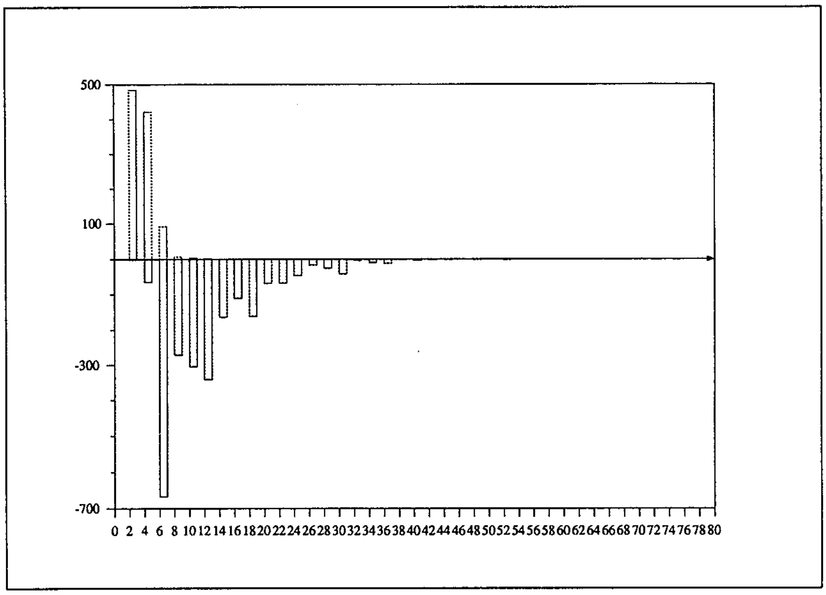

Abbildung 3.3: Für jeden im Intervall $[5, 31627]$ möglichen Abstand zwischen zwei Primzahlen p_ρ und $p_{\rho-1}$ wurde gezählt, wie oft die Vorwärtsdifferenz $\Delta_\rho > 0$ und $\Delta_\rho \leq 0$ ist. Für die Abstände 2 und 4 überwiegen positive Werte von Δ_ρ.

Um diesen Sachverhalt zu verdeutlichen, wurde in der Abbildung 3.3 für jede Vorwärtsdifferenz

$$p_\rho - p_{\rho-1}$$

gezählt, wie oft $\Delta_\rho \geq 0$ und wie oft $\Delta_\rho < 0$ wird. Man sieht, daß das Vorzeichen von Δ_ρ mit dem Abstand aufeinanderfolgender Primzahlen stark korreliert zu sein scheint.

Um die Bedeutung der Vermutung (3.16) zu unterstreichen, formulieren wir den folgenden

Satz 3.3.1 *Sind $(p_j - 2, p_j)$ die letzten Primzahlzwillinge mit $\Delta_\rho < 0$ aber nicht die letzten existierenden Primzahlzwillinge, dann gibt es unendlich viele davon.*

Beweis: Sind die Voraussetzungen des Satzes erfüllt, dann gibt es Primzahlzwillinge $(p_i - 2, p_i)$ mit $p_i > p_j$ und $\Delta_i \geq 0$. Wir setzen $t := \kappa(p_i)$, so daß also $p_i - 2 = 6t - 1$ und $p_i = 6t + 1$ ist. Dieses kann aber nicht das letzte

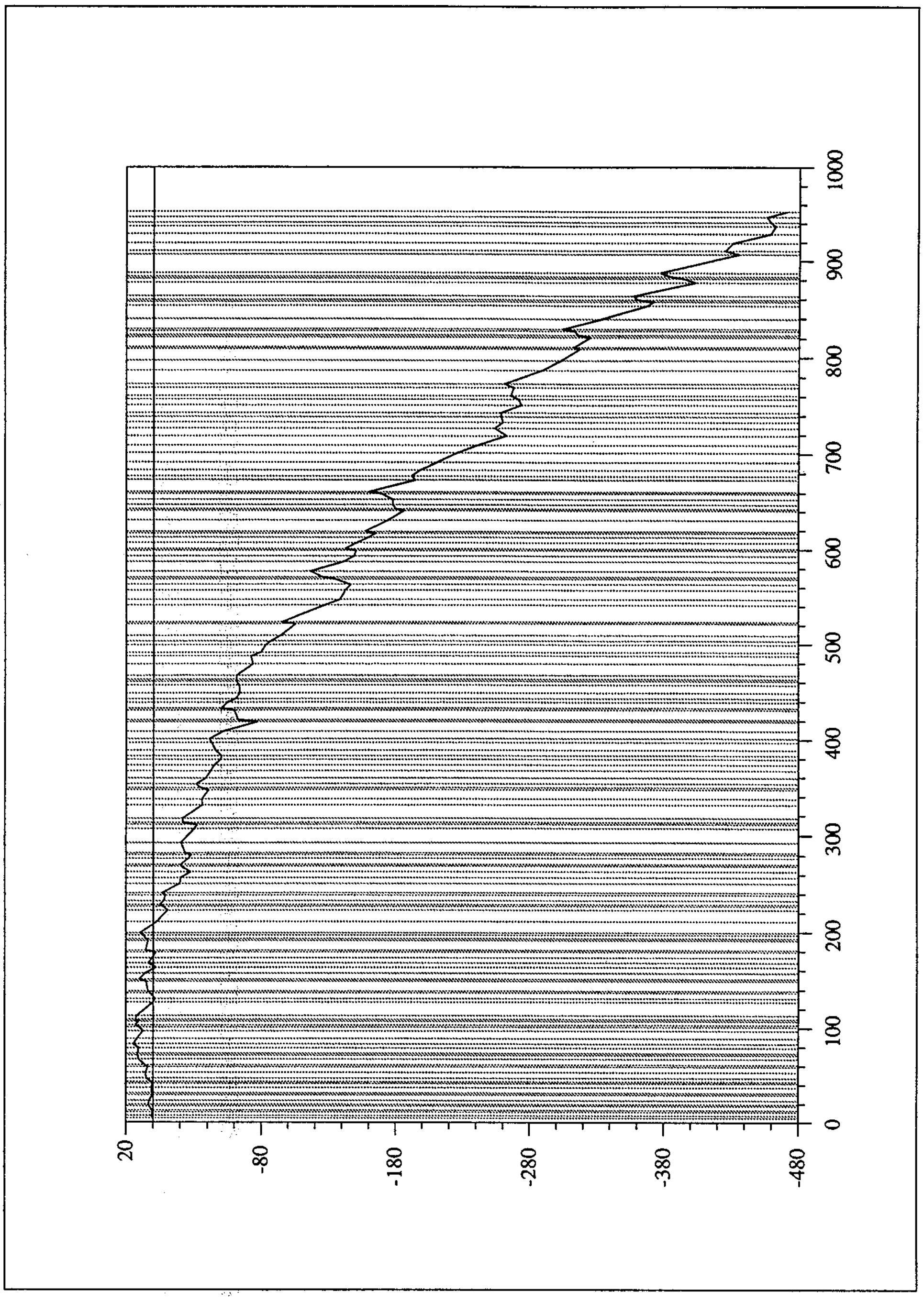

Abbildung 3.4: $\Sigma_\rho^*(\kappa(p^2))$ für die Primzahlen $p = 5, 7, \ldots, 953$ (senkrechte Linien bei der Betrachtung im Querformat).

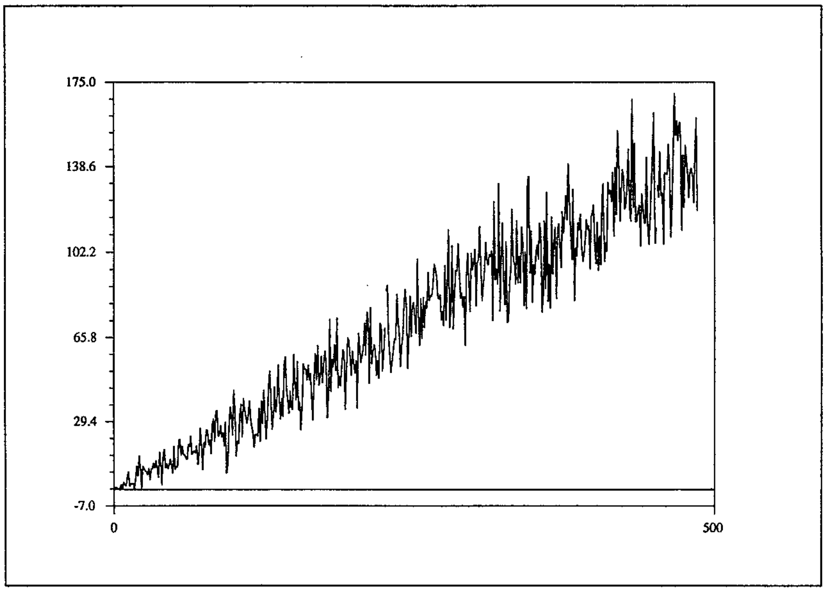

Abbildung 3.5: Δ_j für die ersten 486 Primzahlzwillinge. Kann es jemals wieder in den negativen Bereich zurückkehren?

existierende Zwillingspaar sein, denn wegen (3.12) ist

$$\begin{aligned}
\pi_2(p_i^2) - \pi_2((p_i-2)^2) &= \kappa(p_i^2) \prod_{3<p\leq p_i} \left(1-\frac{2}{p}\right) \\
&\quad -\kappa((p_i-2)^2) \prod_{3<p\leq p_i-2} \left(1-\frac{2}{p}\right) + \Delta_i \\
&= (6t^2+2t)\left(1-\frac{2}{p_i}\right) \prod_{3<p\leq p_i-2} \left(1-\frac{2}{p}\right) \\
&\quad -(6t^2-2t) \prod_{3<p\leq p_i-2} \left(1-\frac{2}{p}\right) + \Delta_i \\
&= \prod_{3<p\leq p_i-2} \left(1-\frac{2}{p}\right)\left(4t-\frac{2t(6t-1)}{6t+1}\right) + \Delta_i \\
&> 2t \prod_{3<p\leq p_i-2} \left(1-\frac{2}{p}\right) \gg 1,
\end{aligned}$$

weil $\Delta_i \geq 0$ ist. Somit müßte es im Intervall $](p_i - 2)^2, p_i^2[$ mindestens einen weiteren Primzahlzwilling $(p_{k-1}, p_k) := (p_k - 2, p_k)$ geben.

□

Bemerkung: Die Richtigkeit der Zwillingsvermutung würde sogar folgen, wenn für alle Primzahlzwillinge $(p_\rho - 2, p_\rho) = (6t - 1, 6t + 1)$ bloß

$$\Delta_\rho \geq -2t \prod_{3<p\leq p_\rho - 2} \left(1 - \frac{2}{p}\right) \tag{3.17}$$

verlangt würde, da dann die Differenz $\pi_2(p_\rho^2) - \pi_2((p_\rho - 2)^2)$ als eine ganze Zahl nicht einen gebrochenen Anteil nahe bei Null bedeuten kann. Der Satz 3.3.1 verschärft zwar diese Forderung, aber vielleicht ist das Feststellen des Vorzeichens von Δ_ρ einfacher (siehe nächster Abschnitt), als der Nachweis der Gültigkeit einer Ungleichung wie (3.17). Außerdem zeigt der Trend in der Abbildung 3.5, daß sich dieser zunächst einmal umkehren müßte, damit die Folge der Primzahlzwillinge überhaupt aufhören kann.

3.4 Entrekursivierung der Formeln für Σ_ρ^* und s_ρ

Die Formelzeile (3.11) bringt Σ_ρ^* in Verbindung mit allen Fourierkoeffizienten $c_\rho(j)$, die wiederum von allen Werten $s_\rho(k)$, $k = 0, \ldots, N - 1$ abhängen. In diesem Abschnitt leiten wir eine Formel her, die diese Abhängigkeit auf alle Teiler von N reduziert. Wir zeigen den

Satz 3.4.1 *Sei p_ρ eine Primzahl > 3 und $N = \prod_{3<p\leq p_\rho} p$. Ferner sei für jeden Teiler $d|N$ die charakteristische Funktion*

$$\sigma_d(l) := \begin{cases} 1, & \textit{falls } (36l^2 \equiv 1 \bmod d) \\ 0 & \textit{sonst} \end{cases} \qquad \forall l \in \mathbb{Z}$$

definiert. Dann gilt

$$\Sigma_\rho^*(n) =$$

$$2 \sum_{d|N} \frac{\mu(d)}{d} \sum_{l=1}^{\frac{d-1}{2}} \sigma_d(l) \sum_{z=1}^{\frac{d-1}{2}} \operatorname{ctg}\left(\frac{\pi z}{d}\right) \sin\left(\frac{2\pi z n}{d}\right) \cos\left(\frac{2\pi z l}{d}\right) \tag{3.18}$$

für alle $n = 0, \ldots, N - 1$.

Beweis: Zur Abkürzung setzen wir

$$D_n(\alpha) := \operatorname{ctg}\left(\frac{\pi\alpha}{2}\right)\sin(n\alpha) \qquad \forall \alpha \neq 2\pi k,\ k \in \mathbb{Z}.$$

Damit ist nach (3.11)

$$\begin{aligned}
\Sigma_\rho^*(n) &= \sum_{j=1}^{\delta} c_\rho(j) D_n\left(\frac{2\pi j}{N}\right) \\
&= \sum_{j=1}^{\delta} \frac{1}{N} \sum_{l=0}^{N-1} s_\rho(l) e\left(\frac{lj}{N}\right) D_n\left(\frac{2\pi j}{N}\right) \\
&= \frac{1}{N} \sum_{j=1}^{\delta} D_n\left(\frac{2\pi j}{N}\right) \sum_{l=0}^{N-1} \sum_{d \mid \operatorname{ggT}(36l^2-1,N)} \mu(d) e\left(\frac{lj}{N}\right) \\
&= \frac{1}{N} \sum_{d \mid N} \mu(d) \sum_{j=1}^{\delta} D_n\left(\frac{2\pi j}{N}\right) \sum_{l=0}^{N-1} \sigma_d(l) e\left(\frac{lj}{N}\right),
\end{aligned}$$

weil σ_d eine d-periodische Folge bildet. Da jedoch $e\left(\frac{lj}{N}\right)$ nicht d-, sondern N-periodisch ist, ist natürlich

$$\sum_{l=0}^{N-1} \sigma_d(l) e\left(\frac{lj}{N}\right) \neq \frac{N}{d} \sum_{l=0}^{d-1} \sigma_d(l) e\left(\frac{lj}{N}\right).$$

Hier muß man genauer rechnen. Für alle $1 \leq j \leq \delta$ gilt

$$\begin{aligned}
\sum_{l=0}^{N-1} \sigma_d(l) e\left(\frac{lj}{N}\right) &= \sum_{m=0}^{N/d-1} \sum_{l=0}^{d-1} \sigma_d(md+l) e\left(\frac{(md+l)j}{N}\right) \\
&= \sum_{l=0}^{d-1} \sigma_d(l) e\left(\frac{lj}{N}\right) \sum_{m=0}^{N/d-1} e\left(\frac{djm}{N}\right) \\
&= (dj \equiv 0 \bmod N) \frac{N}{d} \sum_{l=0}^{d-1} \sigma_d(l) e\left(\frac{lj}{N}\right).
\end{aligned}$$

Die Bedingung $dj \equiv 0(N)$ ist wegen $d|N$ zu $j \equiv 0(N/d)$ äquivalent. Soll j also alle Vielfachen von N/d durchlaufen, die kleiner als δ sind (j läuft von 1 bis δ), in anderen Worten soll $z\frac{N}{d} \leq \delta$ sein für ein $z \in \mathbb{N}$, so folgt

$$z \leq \frac{\delta d}{N} = \frac{N-1}{2} \cdot \frac{d}{N} = \frac{d}{2} - \frac{d}{2N}.$$

Für alle Teiler $d|N$ ist $\frac{d}{2N} \leq \frac{1}{2}$, so daß

$$\frac{d}{2} > \frac{d}{2} - \frac{d}{2N} \geq \frac{d-1}{2}$$

ist. Da alle Teiler $d|N$ ungerade sind, ist $\left[\frac{d}{2}\right] = \frac{d-1}{2}$, so daß die Indexgrenzen $1 \leq z \leq \frac{d}{2} - \frac{d}{2N}$ zu $1 \leq z \leq \frac{d-1}{2}$ äquivalent sind. Damit folgt

$$\begin{aligned} \Sigma_\rho^*(n) &= \frac{1}{N} \sum_{d|N} \mu(d) \sum_{j=1}^{\delta} D_n \left(\frac{2\pi j}{N}\right) (dj \equiv 0(N)) \frac{N}{d} \sum_{l=0}^{d-1} \sigma_d(l) e \left(\frac{lj}{N}\right) \\ &= \sum_{d|N} \frac{\mu(d)}{d} \sum_{z=1}^{(d-1)/2} D_n \left(\frac{2\pi z N}{Nd}\right) \sum_{l=0}^{d-1} \sigma_d(l) e \left(\frac{lzN}{Nd}\right). \end{aligned}$$

Die innere Summe ist in Wirklichkeit reell, da $(\sigma_d)_m$ wegen $36(d-m)^2 - 1 \equiv 36m^2 - 1 \bmod d$ eine gerade Folge ist. Wegen $\sigma_d(0) = 0$ für alle Teiler $d|N$ mit $d > 1$ ist deshalb[9]

$$\sum_{l=0}^{d-1} \sigma_d(l) e \left(\frac{lz}{d}\right) = 2 \sum_{l=1}^{(d-1)/2} \sigma_d(l) \cos \left(\frac{2\pi l z}{d}\right).$$

Durch Einsetzen und erneute Vertauschung der Summationsreihenfolge folgt daraus die Behauptung.

□

Dabei sei darauf hingewiesen, daß die inneren Summen in (3.18) für $d = 1$ leer sind, so daß der dort undefinierte Term $D_n \left(\frac{2\pi z}{d}\right)$ keine Schwierigkeiten macht.

Der Satz 3.3.1 bringt mehr Licht in die Gesetze, die dem Verhalten des Restterms zugrundeliegen. Um das am Anfang des Kapitels gesteckte Ziel wieder aufzugreifen, stellen wir also die folgende komplexe Beziehung zwi-

[9] Da die Kongruenz $36 \cdot 0^2 - 1 \equiv 0 \bmod 1$ offenbar erfüllt ist, gilt im Ausnahmefall $d = 1$ also $\sigma_1(0) = 1$.

schen der Zählfunktion $S(n)$ und n fest:

$$\sum_{k=0}^{n} \sum_{d|\,\mathrm{ggT}(36k^2-1,N)} \mu(d) =$$

$$n \prod_{3<p\leq p_\rho} \left(1-\frac{2}{p}\right) + \frac{1}{2}(1+s_\rho(n)) +$$

$$2\sum_{d|N} \frac{\mu(d)}{d} \sum_{\substack{l=1 \\ 36l^2\equiv 1(d)}}^{(d-1)/2} \sum_{z=1}^{(d-1)/2} \operatorname{ctg}\left(\frac{\pi z}{d}\right) \sin\left(\frac{2\pi z n}{d}\right) \cos\left(\frac{2\pi z l}{d}\right).$$

Die Funktion $\sigma_d(l)$ wurde hier einfach durch die Summationseinschränkung $36l^2 \equiv 1(d)$ ersetzt. Wir wissen aus der Gleichung (3.7) um die asymptotische Entwicklung von $n\tan(\gamma) = n\prod_{3<p\leq p_\rho}(1-2/p)$. Die numerische Auswertung des Restterms zeigt, wie wir gesehen haben, daß dieser "klein" im Vergleich zum Hauptterm ausfällt. Die Formel scheint jedoch zu komplex zu sein, um Aussagen für $p_\rho \to \infty$ machen zu können. Um den Hauptterm und den Restterm noch besser vergleichen zu können, bemerken wir, daß

$$\prod_{3<p\leq p_\rho} \left(1-\frac{2}{p}\right) = 2\sum_{d|N} \frac{\mu(d)}{d} 2^{\omega(d)-1} = 1 + 2\sum_{d|N} \frac{\mu(d)}{d} \sum_{\substack{l=1 \\ 36l^2\equiv 1(d)}}^{(d-1)/2} 1$$

ist wobei die 1 vom Term $\frac{\mu(1)}{1}\sigma_1(0)$ herrührt. Damit haben wir den folgenden Satz bewiesen:

Satz 3.4.2 *Sei p_ρ eine Primzahl > 3 und $N = \prod_{3<p\leq p_\rho} p$. Dann gilt für alle $n = 0, \ldots, N-1$ die Beziehung*

$$\sum_{k=0}^{n} \sum_{d|\,\mathrm{ggT}(36k^2-1,N)} \mu(d) =$$

$$n + \frac{1}{2} + \frac{1}{2}s_\rho(n) + 2\sum_{d|N} \frac{\mu(d)}{d} \sum_{\substack{l=1 \\ 36l^2\equiv 1(d)}}^{(d-1)/2} n +$$

$$2\sum_{d|N} \frac{\mu(d)}{d} \sum_{\substack{l=1 \\ 36l^2\equiv 1(d)}}^{(d-1)/2} \sum_{z=1}^{(d-1)/2} \operatorname{ctg}\left(\frac{\pi z}{d}\right) \sin\left(\frac{2\pi z n}{d}\right) \cos\left(\frac{2\pi z l}{d}\right).$$

Speziell ergibt sich so die Anzahl der Primzahlzwillinge zwischen p_ρ und p_ρ^2, genauer der Ausdruck $\pi(p_\rho^2) - \pi(p_\rho) + \theta_\rho$ mit dem auf Seite 83 definiertem θ_ρ, wenn man rechts für n die Zahl $\kappa(p_\rho^2)$ einsetzt.

□

Wäre die Zwillingsvermutung falsch, also wären etwa $(p_\tau - 2, p_\tau)$ die letzten existierenden Primzahlzwillinge, dann würde die linke Seite für $p_\rho = 5, \ldots, p_\tau - 2$ zuerst steigen, wie in der Abbildung 3.2 zu sehen ist, dann wieder abfallen, um für $p_\rho = p_\tau - 2$ den Wert 2 und dann für alle übrigen unendlich vielen Primzahlen $p_\rho \geq p_\tau$ den konstanten Wert 1 anzunehmen. Dies würde bedeuten, daß sich der Restterm mit dem Hauptterm stets gerade genau wegheben, ungeachtet dessen, aus wie vielen Primzahlen N zusammengesetzt ist, und daß es am Zusammenspiel der Werte von l, für die die Kongruenz von $36l^2 \equiv 1(d)$ lösbar ist, mit den Sinuswerten für das Argument $n = \kappa(p_\rho^2)$ liegt.

Leider weiß man nur sehr wenig über die Verteilung von Nullstellen von Polynomen modulo einer Zahl, um solche Vermutungen entweder widerlegen oder beweisen zu können. Erstaunlich wäre jedoch, daß das "Wegheben" des Hauptterms mit dem Restterm für die Kongruenzlösungen aller Teiler $d|N$ nicht möglich sein sollte, wenn der größte Primfaktor von N die Primzahl p_τ nicht übersteigt, danach aber grundsätzlich für alle größeren N **immer** eintreten würde. Solche Ergebnisse stärken den Verfasser im Glauben an die Primzahlzwillingsvermutung, die hier natürlich nicht bewiesen wurde.

Man könnte nun zur Vermutung (3.16) zurückkehren und versuchen, mit der neuen Formel für Σ_ρ^* ihre Richtigkeit zu beweisen.
Seien $(p_{\rho-1}, p_\rho) = (p_\rho - 2, p_\rho)$ Primzahlzwillinge mit $p_\rho > 5$. Ferner setzen wir wieder $t = \kappa(p_\rho) = \kappa(p_\rho - 2)$. Um zu zeigen, daß $\Sigma_\rho^*(\kappa(p_\rho^2)) - \Sigma_{\rho-1}^*(\kappa(p_{\rho-1}^2)) \geq 0$ ist für hinreichend großes p_ρ müßte man also zeigen[10], daß

$$p_\rho \sum_{d|N} \frac{\mu(d)}{d} \sum_{\substack{l=1 \\ 36l^2 \equiv 1(d)}}^{\frac{d-1}{2}} \sum_{z=1}^{\frac{d-1}{2}} \operatorname{ctg}\left(\frac{\pi z}{d}\right) \sin\left(\frac{2\pi z \overset{(6t^2+2t)}{\cancel{2t}}}{d}\right) \cos\left(\frac{2\pi z l}{d}\right) \geq$$

$$\sum_{d|(N/p_\rho)} \frac{\mu(d)}{d} \sum_{\substack{l=1 \\ 36l^2 \equiv 1(dp_\rho)}}^{\frac{dp_\rho-1}{2}} \sum_{z=1}^{\frac{dp_\rho-1}{2}} \operatorname{ctg}\left(\frac{\pi z}{dp_\rho}\right) \sin\left(\frac{2\pi z(6t^2 - 2t)}{dp_\rho}\right) \cos\left(\frac{2\pi z l}{dp_\rho}\right)$$

[10] dies folgt unmittelbar durch Einsetzen

ist für hinreichend großes[11] p_ρ. Auch hier scheint also die Beweisführung hoffnungslos, obwohl die Abbildung 3.5 für die Richtigkeit dieser Vermutung sprechen würde, die nach Satz 3.3.1 hinreichend für die Richtigkeit der Primzahlzwillingsvermutung ist.

Zum Schluß des Kapitels und dieser Arbeit wird eine ähnliche explizite Darstellung für die charakteristische Funktion $s_\rho(n)$ bewiesen[12].

Satz 3.4.3 *Sei p_ρ eine Primzahl > 3 und $N = \prod_{3<p\leq p_\rho} p$. Ferner sei für $n = 0, \dots, N-1$*

$$\Sigma_\rho^1(n) := 4 \sum_{d|N} \frac{\mu(d)}{d} \sum_{\substack{l=1 \\ 36l^2 \equiv 1(d)}}^{\frac{d-1}{2}} \sum_{z=1}^{\frac{d-1}{2}} \cos\left(\frac{2\pi z l}{d}\right) \cos\left(\frac{2\pi z n}{d}\right).$$

gesetzt. Dann gilt für die charakteristische Funktion

$$s_\rho(n) = \sum_{d|\,\mathrm{ggT}(36n^2-1,N)=1} \mu(d)$$

für $n = 0, \dots, N-1$ die folgende Beziehung:

$$s_\rho(n) = \tan(\gamma) \;+\; \Sigma_\rho^1(n) \tag{3.19}$$

mit der nur von p_ρ abhängigen Konstante

$$\tan(\gamma) := \prod_{3<p\leq p_\rho} \left(1 - \frac{2}{p}\right).$$

Bemerkung: Aus diesem Satz folgt also unmittelbar, daß $\Sigma_\rho^1(n)$ grundsätzlich nur zwei Werte annehmen kann: $1 - \tan(\gamma)$ und $-\tan(\gamma)$.
Insbesondere für $n = 1, \dots, \kappa(p_\rho)$ gilt sicher $\Sigma_\rho^1(n) = -\tan(\gamma)$.
Für $n = \kappa(p_\rho) + 1, \dots, \kappa(p_\rho^2)$ gilt genau dann $\Sigma_\rho^1(n) = 1 - \tan(\gamma)$, wenn die Zahlen $(6n-1, 6n+1)$ Primzahlzwillinge sind.

Wäre die Zwillingsvermutung falsch, dann würde für alle Primzahlen $p_\rho \geq p_\tau$ die Gleichung $\Sigma_\rho^1(n) = -\tan(\gamma)$ gelten für $n = 1, \dots, \kappa(p_\rho^2)$, wenn $(p_\tau - 2, p_\tau)$ die letzten existierenden Zwillinge sind.

[11] $p_\rho > 463$?
[12] vgl. Definition auf Seite 82

Beweis: Wir müssen nur die Aussage (3.19) beweisen. Der Beweis besteht im Wesentlichen in der Entrekursivierung der Formel (3.13). Danach und dem Satz 3.4.1 gilt

$$\begin{aligned} s_\rho(n+1) &= 2\tan(\gamma) - s_\rho(n) + 2\Sigma^*_\rho(n+1) - 2\Sigma^*_\rho(n) \\ &= 2\tan(\gamma) - s_\rho(n) + \Sigma^1_\rho(n+1) + \Sigma^1_\rho(n), \end{aligned} \tag{3.20}$$

weil in den auftauchenden inneren Summen die folgende Umformung stattfindet:

$$\begin{aligned} &\operatorname{ctg}\left(\frac{\pi z}{d}\right)\cos\left(\frac{2\pi zl}{d}\right)\left(\sin\left(\frac{2\pi z(n+1)}{d}\right) - \sin\left(\frac{2\pi zn}{d}\right)\right) = \\ &\quad 2\operatorname{ctg}\left(\frac{\pi z}{d}\right)\cos\left(\frac{2\pi zl}{d}\right)\cos\left(\frac{\pi z(2n+1)}{d}\right)\sin\left(\frac{\pi z}{d}\right) = \\ &\quad 2\cos\left(\frac{\pi z}{d}\right)\cos\left(\frac{2\pi zl}{d}\right)\cos\left(\frac{\pi z(2n+1)}{d}\right) \\ &\quad \cos\left(\frac{2\pi zl}{d}\right)\left(\cos\left(\frac{2\pi zn}{d}\right) + \cos\left(\frac{2\pi z(n+1)}{d}\right)\right). \end{aligned}$$

Wir brauchen nun die für alle $n \in \mathbb{Z}$ definierte Hilfsfunktion

$$odd(n) := \begin{cases} 1, & \text{falls } n \text{ ungerade} \\ 0 & \text{sonst.} \end{cases}$$

Aus der Gleichung (3.20) folgt damit induktiv die folgende Beziehung:

$$s_\rho(n) = odd(n) 2\tan(\gamma) + (-1)^n(1 - \Sigma^1_\rho(0)) + \Sigma^1_\rho(n). \tag{3.21}$$

Für $n = 0$ gilt nämlich

$$s_\rho(0) = 1 - \Sigma^1_\rho(0) + \Sigma^1_\rho(0) = 1.$$

Sei nun die Behauptung (3.19) für alle $m = 0, \ldots, n$ erfüllt. Dann gilt nach (3.20)

$$\begin{aligned} s_\rho(n+1) &= 2\tan(\gamma) - s_\rho(n) + \Sigma^1_\rho(n+1) + \Sigma^1_\rho(n) \\ &= 2\tan(\gamma) - odd(n) 2\tan(\gamma) - (-1)^n(1 - \Sigma^1_\rho(0)) \\ &\quad - \Sigma^1_\rho(n) + \Sigma^1_\rho(n+1) + \Sigma^1_\rho(n) \\ &= odd(n+1) 2\tan(\gamma) + (-1)^{n+1}(1 - \Sigma^1_\rho(0)) + \Sigma^1_\rho(n+1). \end{aligned}$$

Als letztes bleibt noch zu zeigen, daß

$$odd(n) 2\tan(\gamma) + (-1)^n(1 - \Sigma^1_\rho(0)) = \tan(\gamma) \qquad \forall n \in \mathbb{Z}$$

ist, was für alle $n \in \mathbb{Z}$ nur erfüllt sein kann, wenn die Gleichung

$$\Sigma_\rho(0) = 1 - \tan(\gamma) \tag{3.22}$$

richtig ist. Dies ist ein Spezialfall der Gleichung

$$\Sigma_\rho(n) = 2\sum_{j=1}^{\delta} c_\rho(j) \cos\left(\frac{2\pi jn}{N}\right) \tag{3.23}$$

wenn, wie schon früher, $\delta = (N-1)/2$ gesetzt wird und $c_\rho(j)$ die diskreten Fourierkoeffizienten aus (3.3) bezeichnen. Die Gleichung (3.22) folgt dann unmittelbar aus dem Ergebnis (3.8).

Um nun noch (3.23) zu beweisen, reicht es, die Rechnung in diesem Beweis für die Definition von $\Sigma^*_\rho(n)$ aus (3.11) zu wiederholen, was auf die Gleichung

$$\begin{aligned} s_\rho(n) &= odd(n) 2\tan(\gamma) + (-1)^n(1 - 2\sum_{j=1}^{\delta} c_\rho(j)) \\ &\quad + 2\sum_{j=1}^{\delta} c_\rho(j) \cos\left(\frac{2\pi jn}{N}\right) \end{aligned}$$

führt. Der Vergleich mit (3.21) liefert schließlich

$$s_\rho(n) = \tan(\gamma) + 2\sum_{j=1}^{\delta} c_\rho(j) \cos\left(\frac{2\pi jn}{N}\right) = \tan(\gamma) + \Sigma^1_\rho(n).$$

□

Literaturverzeichnis

[1] **Aigner, M.; Ziegler, G.M.:** *„Proofs from THE BOOK“*. Springer-Verlag, (Berlin, Heidelberg, u.a.), 1998

[2] **Ankeny, N.C.; Onishi, H.:** *„The general sieve“*. Acta Arith. 10, (MR 29, 4740), 1964/1965

[3] **Batut, C.; Belabas, K.; Bernardi, D.; Cohen, H.; Olivier, M.:** *„User's Guide to PARI-GP“*. http://hasse.mathematik.tu-muenchen.de/ntsw/pari/, (Université Bordeaux), Mai 1999

[4] **Bauer, J.-P.:** *„Sur un problème equivalent au problème des nombres premieres jumeaux“*. Ann. Sci. Math (4), No.2, (Univ. Franche-Comté Besançon), 1990

[5] **Brüdern, J.:** *„Einführung in die analytische Zahlentheorie“*. Springer-Verlag, (Berlin, Heidelberg), 1995

[6] **Brun, V.:** *„La serie* $1/5+1/7+\dots$ *ou le dénominateurs sont nombres premiers jumeaux et convergente ou finie“*. Bull. Sci.Math 43, S. 124-128, (Frankreich), 1919

[7] **Brun, V.:** *„Le crible d'Eratosthène et le théorème de Goldbach“*. C.R. Acad. Sci. S. 544-546, (Paris), 1919

[8] **Buchstab, A.A.:** *„Asymptotic estimates of a general number-theoretic function“*. Russisch, Mat. Sbornik 2 (44), S. 1239-1246, (UDSSR), 1937

[9] **Buchstab, A.A.:** *„New results in the investigation of the Goldbach-Euler problem and the problem of prime pairs“*. Russisch, Dokl. Akad. Nauk 162, S. 735-738, (UDSSR), 1965

[10] **Buchstab, A.A.:** *„Combinatorial intensification of the sieve method of Eratosthenes"*. Russisch, Uspehi Matematiceskich Nauk 22, no. 3 (135). S. 199-226, (UDSSR), 1967

[11] **Butz, T.:** *„Fouriertransformation für Fußgänger"*. B.G. Teubner-Verlag, (Stuttgart, Leipzig), 1998

[12] **Caldwell, Ch.K.:** *„The Largest Known Primes"*. http://www.utm.edu/research/primes/largest.html, (Internet), 1999

[13] **Chen, Jing-run:** *„On the representation of a large even number as the sum of a prime and the product of at most two primes"*. Sci. Sinica 16, S.157-176, (), 1973

[14] **Cipra, B:** *„How Number Theory Got the Best of the Pentium Chip"*. Science 267, S. 175, (USA), 1995

[15] **Dirichlet, J.P.G.:** *„Beweis des Satzes, daß jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Faktor sind, unendlich viele Primzahlen enthält"*. Abh. Akad. S.45-47, (Berlin), 1837

[16] **Euler, L.:** *„Introduction in Analysis Infinitorum, Tomus Primus"*. Opera Omnia, Ser. 1, Vol. 90, (Lausanne), 1748

[17] **Fouvry, E. Tanenbaum, G.:** *„Entiers sans grand facteur premier en progressions arithmétique"*. Proc. London Math. Soc (3) 63, S. 449-494, (London), 1991

[18] **Graham, R.L.; Knuth, D.E.; Patashnik O.:** *„Concrete Mathematics"*. Addison-Wesley Publ. Comp., (USA, Canada), 1989

[19] **Halberstam, H; Richert, H.-E.:** *„Sieve Methods"*. Academic Press, (London, New York, San Francisco), 1974

[20] **Halberstam, H; Roth, K.F.:** *„Sequences"*. Oxford at the Clarendon Press, (Glasgow, New York u.a.), 1966

[21] **Hardy, G.H.; Littlewood, J.E.:** *„Some problems of Partition Numerorum III: On the expression of a number as a sum of primes"*. Acta Mathematica 44, (S.1-70), 1923

[22] **Hardy G.H.; Wright E.M.:** *„Einführung in die Zahlentheorie“.* Deutsche Übersetzung des Originals „An Introduction to the Theory of Numbers“, R. Oldenbourg, (München), 1958

[23] **Hooley, C.:** *„Applications of sieve methods to the theory of numbers“.* Cambridge University Press, (Cambridge, London, New York, Melbourne), 1976

[24] **Jerri, A.J.:** *„Integral And Discrete Transforms With Applications And Error Analysis“.* , (New York, Basel, Hong Kong), 1992

[25] **Jones, G.A.; Jones J.M.:** *„Elementary Number Theory, SUMS“.* Springer-Verlag, (London), 1998

[26] **Krätzel E.:** *„Zahlentheorie“.* VEB Deutscher Verlag der Wissenschaften, (Jena), 1981

[27] **Kuhn, P.:** *„Zur Viggo Brun'schen Siebmethode“.* Norske Vid. Selsk. Forh. Trondhjem 14, (no. 39), 1941

[28] **Landau, E.:** *„Aus der elementaren und additiven Zahlentheorie, I.Band“.* Verlag von S. Hirzel, (Leipzig), 1927

[29] **Nycely, T.:** *„Enumeration to* 10^{14} *of the Twin Primes and Brun's Constant“.* Virginia J. Sci. 46, S.195-204, (USA), 1996

[30] **Porter, J.W.:** *„Some numerical results in the Selberg sieve method“.* Acta Arith. 20, (MR 46, 5268), 1972

[31] **Prachar, K.:** *„Primzahlverteilung“.* Springer-Verlag, Reprint, (Berlin, Heidelberg, New York), 1978

[32] **Prachar, K.:** *„On integers having many representations as a sum of two primes“.* J. Lond. math. Soc. 29, S. 347-350, (London), 1953

[33] **Rényi, A.:** *„Über die Darstellung gerader Zahlen als Summe einer Primzahl und einer Fastprimzahl“.* (Russisch) S.57-78, Akademia Nauk, 12, (UDSSR), 1947

[34] **Schwarz, W.:** *„Einführung in Methoden und Ergebnisse der Primzahltheorie“.* Bibliogr. Institut AG, (Mannheim, Wien, Zürich), 1969

[35] **Schwarz, W.:** *„Einführung in Siebmethoden der analytischen Zahlentheorie“*. B.I.-Wissenschaftsverlag, (Mannheim, Wien, Zürich), 1974

[36] **Selberg, A.:** *„On the normal density of primes in small intervalls and the difference between consecutive primes“*. Arch. Math. Naturvid. 47, no. 6, S. 87-105, (Norwegen), 1943

[37] **Sheyser, M.:** *„Prime numbers and the* $6N \pm 1$ *series“*. Math. Sci. 18, (Nr.2, S.134-136), 1993

[38] **Sierpiński, W.:** *„Über die Summation der Reihe* $\sum p_n 10^{-2^n}$ *“*. (Polnisch) Prace math. fiz. 18, S.1-60, (Polen), 1907

[39] **Tchebycheff, P.L.:** *„Recherches nouvelles sur les nombres premieres, S.397-401, 738-739“*. CR Paris 29, (Paris), 1851

[40] **Vinogradoff, I.:** *„Über die Darstellung einer ungeraden Zahl als Summe dreier Primzahlen“*. (Russisch) S.139-142, Akademia Nauk, 16, (UDSSR), 1937

[41] **Wolf M.:** *„Some conjectures on the gaps between consecutive primes“*. http://violet.ift.uni.wroc.pl/~mwolf, (Internet), 1995