Einführung in die

Additive Zahlentheorie

Vorlesung im Wintersemester 2007/08
an der Albert-Ludwigs-Universität Freiburg

Karin Halupczok

Freiburg, den 15. Februar 2008
korrigierte Endfassung vom 22. April 2008

Inhaltsverzeichnis

§ 0 Einleitung

Additive Zahlentheorie ist derjenige Zweig der Zahlentheorie, der die Darstellungen und Darstellbarkeit natürlicher Zahlen als Summen ganzer Zahlen aus bestimmten Mengen untersucht. Ist eine Menge $\mathcal{A} \subseteq \mathbb{Z}$, etwa eine Folge

$$\mathcal{A} = \{a_1 < a_2 < a_3 < \dots\}$$

ganzer Zahlen gegeben, wird oft die Frage gestellt, welche natürliche Zahlen als Summe einer festen Anzahl von Elementen aus $\mathcal{A}$ dargestellt werden können. Für ein festes $s \in \mathbb{N}$ sind also diejenigen natürlichen Zahlen n gesucht, für die die diophantische Gleichung

$$x_1 + x_2 + \dots + x_s = n \tag{1}$$

eine Lösung in $x_1, \dots, x_s \in \mathcal{A}$ besitzt.

Die Zahlenmenge $\mathcal{A}$ kann allgemein beschrieben sein (z.B. nur dadurch daß sie „viele“ Elemente besitzt), oder eine bestimmte Menge von gewissen arithmetischen Interesse sein (z. B. die Menge der k-ten Potenzen, der Primzahlen, der Werte eines Polynoms $F \in \mathbb{Z}[x]$ an den natürlichen Zahlen oder an den Primzahlen). Probleme der letzteren Art rechnet man der „additiven Primzahltheorie“ zu, aber man kann auch Probleme mit „Mischformen“ behandeln, d. h. die Lösbarkeit obiger diophantischer Gleichung (1) in $x_i \in \mathcal{A}_i, i = 1, \dots, n$, sofern n viele Mengen $\mathcal{A}_i$ vorgegeben sind.

Wir nennen nun eine Menge $\mathcal{A} \subseteq \mathbb{N}_0$ eine **Basis bezüglich** $h \in \mathbb{N}$, falls jede natürliche Zahl n als Summe von h vielen (nicht notwendig verschiedenen) Elementen von $\mathcal{A}$ geschrieben werden kann, d. h. falls $\forall\, n \in \mathbb{N}\ \exists\, x_1, \dots, x_h \in \mathcal{A}:\ n = x_1 + \dots + x_h$ gilt.
$\mathcal{A}$ heißt **Basis (von endlicher Ordnung)**, falls es ein $h \in \mathbb{N}$ gibt, so daß $\mathcal{A}$ eine Basis bezüglich h ist. Das kleinste solche h nennen wir die **Ordnung** der Basis $\mathcal{A}$.

Nehmen wir als Beispiel für $\mathcal{A}$ etwa die Menge der Quadratzahlen

$$\mathcal{A} = \{1^2, 2^2, 3^2, \dots\},\ \text{kurz „Quadrate“ bzw. „}\square\text{“}.$$

Der Vierquadratesatz von Lagrange besagt gerade, daß $\mathcal{A}$ eine Basis bezüglich 4 ist. Der Eulersche Zweiquadratesatz gibt genaue Auskunft darüber, welche natürlichen Zahlen als Summe zweier Quadrate geschrieben werden können, nämlich *genau* die $n \in \mathbb{N}$, in deren Primfaktorzerlegung alle Primteiler p von n mit $p \equiv 3\ (4)$ in gerader Potenz auftreten. (Das sind z. B. die Quadratzahlen.)

$\mathcal{A}$ ist also keine Basis der Ordnung 2, und daß $\mathcal{A}$ auch keine der Ordnung 3 ist, besagt der Dreiquadratesatz, den wir in § 2 der Vorlesung vollständig beweisen werden.
(Die einfachere Richtung dieses Satzes, nämlich daß die Zahlen $n = 4^a(8b+7), a, b \in \mathbb{N}_0$, *nicht* Summe dreier Quadrate sind, haben wir in der elementaren Zahlentheorie schon gesehen.)

Demnach ist die Menge $\mathcal{A}$ der Quadrate eine Basis der Ordnung 4.

Als Verallgemeinerung können wir für $\mathcal{A}$ die Menge der k–ten Potenzen nehmen, d. h.

$$\mathcal{A} = \{1^k, 2^k, 3^k, \dots\}, \quad k \geq 2.$$

Ob diese Menge stets eine Basis endlicher Ordnung ist, ist bekannt als das **Waringsche Problem**. Dessen Lösung werden wir in § 4 angehen und dafür Methoden einsetzen, die uns aus § 3 dann schon bekannt sein werden.

Der § 3 behandelt die sogenannte Goldbachsche Vermutung, die in einem Teil lautet, daß jede ungerade Zahl ≥ 7 die Summe dreier Primzahlen ist („ternäre Goldbachsche Vermutung"). Daß dies für alle sehr großen ungeraden Zahlen stimmt, wurde 1937 von Vinogradov bewiesen; den Beweis mit der Kreismethode von Hardy und Littlewood werden wir ausführlich behandeln. Der zweite Teil der Goldbachschen Vermutung besagt, daß jede gerade Zahl ≥ 4 Summe zweier Primzahlen ist („binäre Goldbachsche Vermutung"), und ist bis heute ein ungelöstes Problem.

In § 5 lernen wir noch einige weitere Varianten des Waringschen und Goldbachschen Problems ausführlich kennen, sowie in § 6 einige – teils sehr aktuelle – Forschungsergebnisse zu diversen additiven Problemen. In letzterem werden wir diese nur vorstellen und keine ausführlichen Beweise bringen können.

In § 7 wird ein Überblick über den Beweis des Satzes von Chen gegeben, die bislang beste bekannte Approximation an die binäre Goldbachsche Vermutung. Diese besagt, daß jede hinreichend große gerade natürliche Zahl n als Summe einer Primzahl $p \neq 2$ und einer weiteren natürlichen Zahl P_2 geschrieben werden kann, die aus höchstens zwei Primfaktoren besteht, d. h. also $\forall\, n \geq n_0,\ 2 \,|\, n : n = p + P_2,$ mit $p \neq 2$ prim, $\Omega(P_2) \leq 2$.

In § 1 bringen wir zunächst eine Zusammenfassung über die wichtigsten Ergebnisse der Theorie der Primzahlverteilung der analytischen Zahlentheorie, auf die wir immer wieder als Hilfsmittel zurückgreifen werden: der Primzahlsatz und die Riemannsche Vermutung, Primzahlsätze in arithmetischen Progessionen und Exponentialsummen. Alle anderen Methoden entwickeln wir dann „unterwegs".

§ 1 Die Theorie der Primzahlverteilung

§ 1.1. Der Primzahlsatz und die Riemannsche Vermutung

Das erste Ergebnis zur Primzahlverteilung ist der Satz von Euklid, nämlich daß es unendlich viele Primzahlen gibt. Im Jahr 1798 vermutete Legendre, daß die Primzahlzählfunktion

$$\pi(x) := \#\{p \le x\}$$

der asymptotischen Formel

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1 \qquad \text{(PZS)}$$

genügt – man nennt diese Behauptung den **Primzahlsatz**. Äquivalent formuliert:

$$\pi(x) = \frac{x}{\log x}(1+\mathrm{o}(1)) \text{ bzw. } \pi(x) = \frac{x}{\log x} + \mathrm{o}\Big(\frac{x}{\log x}\Big) \text{ für } x \to \infty.$$

Danach werden die Primzahlen mit wachsendem x immer seltener, bis x machen diese nur einen Anteil von $\frac{1}{\log x}$ aus, was mit wachsendem x gegen 0 geht: die (asymptotische) Dichte der Primzahlen ist also $= 0$. Gauß beobachtete später[1] anhand numerischer Berechnungen, daß das logarithmische Integral

$$\mathrm{li}(x) := \int_2^x \frac{dt}{\log t}$$

ebenso wie $\frac{x}{\log x}$ eine Approximation an $\pi(x)$ ist, d. h. daß $\pi(x) = \mathrm{li}(x)(1+\mathrm{o}(1))$ ist.
Das läßt sich auch so einsehen: Ist $\mathrm{li}(x)$ eine Approximation an $\pi(x)$, so ist auch $\frac{x}{\log x}$ eine solche und umgekehrt, denn durch sukzessive partielle Integration sieht man, daß

$$\begin{aligned}\mathrm{li}(x) = \int_2^x \frac{d}{dt}(t)\cdot\frac{dt}{\log t} &= \frac{t}{\log t}\Big|_2^x + \int_2^x \frac{dt}{\log^2 t} = \dots \\ &= \Big(\frac{t}{\log t} + \frac{t}{\log^2 t} + \frac{2!\,t}{\log^3 t} + \dots + \frac{(N-1)!\,t}{\log^N t}\Big)\Big|_2^x + N!\int_2^x \frac{dt}{\log^{N+1} t} \\ &= \frac{x}{\log x} + \frac{1!x}{\log^2 x} + \dots + \frac{(N-1)!x}{\log^N x} + \mathrm{O}\Big(\frac{x}{\log^{N+1} x}\Big),\end{aligned}$$

weswegen sich $\mathrm{li}(x)$ und $\frac{x}{\log x}$ nur um $\mathrm{O}\big(\frac{x}{\log^2 x}\big)$ unterscheiden.

[1] Gauß schrieb am Heiligabend 1849, daß er im Alter von 15 oder 16 Jahren fand, daß um x die Primzahlen mit Dichte $\approx \frac{1}{\log x}$ auftreten. Somit ist $\pi(x) \approx \sum_{n=2}^{\lfloor x\rfloor} \frac{1}{\log n} \approx \int_2^x \frac{dt}{\log t}$.

Die letzte Abschätzung sieht man so: Es ist

$$\int_2^x \frac{dt}{\log^{N+1} t} = \int_2^{x^{1/2}} \frac{dt}{\log^{N+1} t} + \int_{x^{1/2}}^x \frac{dt}{\log^{N+1} t}$$
$$\ll x^{1/2} + (x - x^{1/2}) \frac{1}{\log^{N+1}(x^{1/2})} \ll \frac{x}{\log^{N+1} x}.$$

Nun stellt man anhand numerischer Werte fest, daß $\mathrm{li}(x)$ eine viel bessere Approximation an $\pi(x)$ ist als $\frac{x}{\log x}$, d. h. man beobachtet, daß die Differenz $|\mathrm{li}(x) - \pi(x)|$ stets kleiner ausfällt als $|\frac{x}{\log x} - \pi(x)|$. In diesem Zusammenhang geben wir die folgende (aktuelle) Tabelle an, die Werte von $\pi(x)$ mit denen von $\mathrm{li}(x)$ vergleicht:

x	$\pi(x) := \#\{p \le x\}$	$\mathrm{li}(x) - \pi(x)$
10^8	5761455	753
10^9	50847534	1700
10^{10}	455052511	3103
10^{11}	4118054813	11587
10^{12}	37607912018	38262
10^{13}	346065536839	108970
10^{14}	3204941750802	314889
10^{15}	29844570422669	1052618
10^{16}	279238341033925	3214631
10^{17}	2623557157654233	7956588
10^{18}	24739954287740860	21949554
10^{19}	234057667276344607	99877774
10^{20}	2220819602560918840	222744643
10^{21}	21127269486018731928	597394253
10^{22}	201467286689315906290	1932355207
10^{23}	1925320391606803968923	7250186214

Anhand der Werte für $\mathrm{li}(x) - \pi(x)$ läßt sich ablesen, daß der Fehler dieser Approximation sogar etwa nur so groß wie $x^{1/2}$ sein müsste. Wir werden auf diese Frage nochmals zurückkommen. Weiter ist die Differenz $\mathrm{li}(x) - \pi(x)$ in dieser Tabelle immer positiv. Das ist nicht immer so: 1914 bewies Littlewood, daß die Differenz unendlich oft ihr Vorzeichen wechselt, und 1986 bewies Te Riele, daß es mehr als 10^{180} aufeinanderfolgende n mit

$\pi(n) > \mathrm{li}(n)$ zwischen $6.62 \cdot 10^{370}$ und $6.69 \cdot 10^{370}$ gibt.

Der erste Schritt in Richtung Beweis des Primzahlsatzes gelang Tschebytschev um 1850, der die Existenz von Konstanten $c_2 > c_1 > 0$ mit

$$\frac{c_1 x}{\log x} \leq \pi(x) \leq \frac{c_2 x}{\log x}$$

zeigte (s. elementare Zahlentheorie). Dabei stellt sich auch heraus, daß es technisch einfacher ist, mit den Tschebytschev-Funktionen

$$\psi(x) = \sum_{n \leq x} \Lambda(n) = \sum_{p^k \leq x} \log p$$

und

$$\vartheta(x) = \sum_{p \leq x} \log p$$

statt mit π zu arbeiten – mit den Funktionen ψ und ϑ lautet der Tschebytschev–Satz einfacher $c_3 x \leq \psi(x) \leq c_4 x$ bzw. $c_5 x \leq \vartheta(x) \leq c_6 x$, und die π–Version ist leicht aus den Abschätzungen für ψ oder ϑ zu gewinnen. Auch für den Primzahlsatz hat man einfacher zu formulierende äquivalente Versionen, diese lauten

$$\lim_{x \to \infty} \frac{\psi(x)}{x} = 1 \quad \Leftrightarrow \quad \psi(x) = x + \mathrm{o}(x)$$

und

$$\lim_{x \to \infty} \frac{\vartheta(x)}{x} = 1 \quad \Leftrightarrow \quad \vartheta(x) = x + \mathrm{o}(x).$$

Im Jahr 1859 fand Riemann einen engen Zusammenhang zwischen $\pi(x)$ und einer bestimmten analytischen Funktion, die heute seinen Namen trägt: die **Riemannsche Zeta–Funktion**, die auf der komplexen Ebene für $s \in \mathbb{C}, \mathrm{Re}\, s > 1$, durch

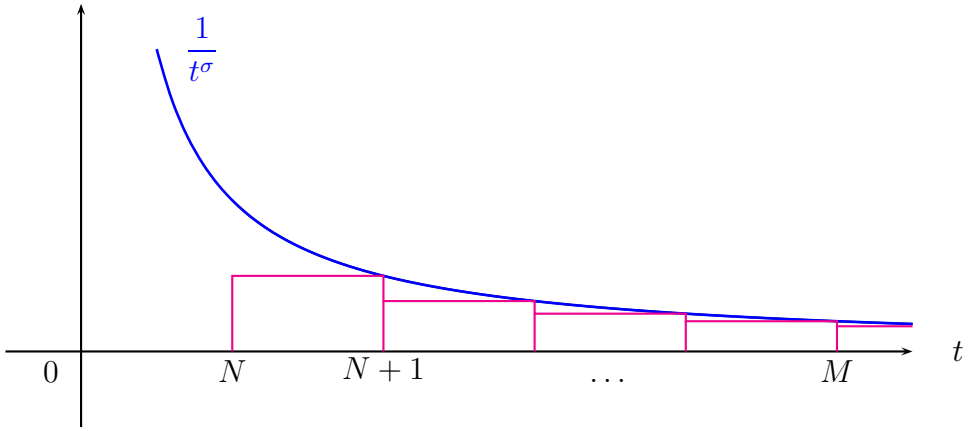
$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$$

definiert ist und eindeutig zu einer holomorphen Funktion auf $\mathbb{C}\backslash\{1\}$ fortgesetzt werden kann – allerdings nicht bei $s = 1$, wo die Funktion einen einfachen Pol besitzt. Die Funktion ζ muß bei $s = 1$ divergieren, denn für $s = 1$ erhält man für die definierende Reihe gerade die harmonische Reihe $\sum_{n=1}^{\infty} \frac{1}{n}$, die bekanntlich divergiert. Für $\sigma := \mathrm{Re}\, s > 1$ ist die definierende Reihe aber konvergent, wie man an dem Integralvergleich

$$\Big| \sum_{n=N+1}^{M} \frac{1}{n^s} \Big| \leq \sum_{n=N+1}^{M} \frac{1}{n^\sigma} \leq \int_N^M \frac{1}{t^\sigma} dt = \frac{1}{1-\sigma} t^{-\sigma+1} \Big|_N^M$$

$$= \frac{1}{1-\sigma}\left(\frac{1}{M^{\sigma-1}} - \frac{1}{N^{\sigma-1}}\right) \longrightarrow_{M,N\to\infty} \quad 0$$

sieht.



Für $s \in \mathbb{C}\backslash\{1\}$, $\operatorname{Re} s \leq 1$, hat man andere Darstellungen für die Zeta-funktion – die Reihe divergiert dort nämlich.

Schon Euler hatte diese Funktion mit rellen Argumenten untersucht und dabei die Produktformel

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}}, \quad \operatorname{Re} s > 1,$$

entdeckt, die bereits einen Zusammenhang von ζ mit den Primzahlen herstellt. Man nennt dieses Produkt daher auch das **Euler–Produkt** für ζ. Die bemerkenswerte Formel $\zeta(2) = \pi^2/6$ geht ebenso auf Euler zurück. Euler zeigte weiter, daß

$$\zeta(2n) = \frac{(-1)^{n-1} B_{2n}}{2(2n)!}(2\pi)^{2n}$$

mit den Bernoullizahlen B_{2n} gilt, die über die Formel

$$\frac{z}{e^z - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!}\, z^n \quad \text{definiert sind.}$$

Für $\zeta(2n+1)$ ist keine solche Formel bekannt.

Riemann entdeckte nun, daß sich im (sogenannten kritischen) Streifen $0 \leq \operatorname{Re} s \leq 1$ unendlich viele Nullstellen der ζ–Funktion befinden, und setzte Vermutungen über deren Lage in Beziehung mit dem Primzahlsatz.

Die berühmteste und bis heute die einzige ungelöste dieser Vermutungen ist bekannt als die **Riemannsche Vermutung (RH)**, welche besagt, daß alle Nullstellen von ζ

im Streifen $0 \le \operatorname{Re} s \le 1$ tatsächlich auf der Geraden $\operatorname{Re} s = \frac{1}{2}$ liegen. Die anderen Probleme der Arbeit Riemanns von 1859 wurden bis Ende des 19. Jahrhunderts gelöst. Insbesondere wurde gezeigt, daß der Primzahlsatz aus dem Nichtverschwinden von ζ auf der Geraden $\operatorname{Re} s = 1$ folgt. Als 1896 Hadamard und de la Vallée–Poussin unabhängig voneinander zeigten, daß tatsächlich $\zeta(1+it) \neq 0$ für alle $t \in \mathbb{R}$ gilt, war damit der Primzahlsatz endgültig bewiesen.

Mit der Untersuchung nullstellenfreier Gebiete nahe $\operatorname{Re} s = 1$ konnte daraufhin der Primzahlsatz mit der Fehlerabschätzung

$$\psi(x) = x + \mathrm{O}\big(x \exp(-C(\log x)^{1/2})\big)$$

bzw. in der π-Version

$$\pi(x) = \operatorname{li}(x) + \mathrm{O}\big(x \exp(-C(\log x)^{1/2})\big)$$

angegeben werden.

Das bislang beste Ergebnis ist

$$\psi(x) = x + \mathrm{O}\big(x \exp(-c(\log x)^{3/5}(\log\log x)^{-1/5})\big)$$

von Vinogradov und Korobov (unabhängig voneinander) aus dem Jahr 1958 und konnte in den letzten 50 Jahren nicht weiter verbessert werden.
Worin nun der fundamentale Zusammenhang zwischen den Primzahlen und den kritischen Nullstellen der ζ–Funktion besteht, wird besonders deutlich durch die sogenannte **explizite Formel**

$$\psi(x) = x - \sum_{\rho, |\operatorname{Im}\rho| \le T} \frac{x^\rho}{\rho} + \mathrm{O}\Big(\frac{x}{T}\log^2 x\Big),$$

gültig für alle $2 \le T \le x$. Die Summe hierin erstreckt sich über alle Nullstellen ρ von ζ im kritischen Streifen, für die $|\operatorname{Im}\rho| \le T$ gilt. Wie viele kritische Nullstellen ρ mit $|\operatorname{Im}\rho| \le T$ gibt es nun? Bezeichnet $N(T)$ deren Anzahl (mehrfache Nullstellen zählen dabei gemäß ihrer Vielfachheit), so gilt der Satz, daß

$$N(T+1) - N(T) = \mathrm{O}(\log T) \quad \text{und} \quad N(T) = \frac{T}{2\pi}\log\Big(\frac{T}{2\pi}\Big) - \frac{T}{2\pi} + \mathrm{O}(\log T).$$

(Insbesondere hat ein $\rho = \beta + i\eta$ mit $\eta \ge 2$ die Vielfachheit $\mathrm{O}(\log\eta)$.)
Unter Annahme der Riemannschen Vermutung $\operatorname{Re}\rho = \frac{1}{2}$ für alle kritischen Nullstellen ρ von ζ gilt der Primzahlsatz in der scharfen Form

$$\psi(x) = x + \mathrm{O}\big(x^{1/2}\log^2 x\big), \text{ unter (RH)},$$

bzw.

$$\pi(x) = \operatorname{li}(x) + \mathrm{O}\big(x^{1/2}\log x\big), \text{ unter (RH)}.$$

Diese läßt sich leicht aus obiger expliziter Formel ableiten: Zum Beweis setzen wir darin $T := x^{1/2}$ (≥ 2 für $x \geq 4$) und erhalten für die ρ–Summe so

$$\begin{aligned}\sum_{\rho,|\operatorname{Im}\rho|\leq T} x^{1/2}|\rho|^{-1} &= \mathrm{O}\Big(x^{1/2} \sum_{1\leq n\leq \lfloor T\rfloor} \frac{1}{n} \underbrace{\#\{\rho, n < |\operatorname{Im}\rho| \leq n+1\}}_{N(n+1)-N(n)}\Big)\\ &= \mathrm{O}\Big(x^{1/2} \sum_{n\leq \lfloor T\rfloor} \frac{\log n}{n}\Big) \quad \text{nach obigem}\\ &= \mathrm{O}\big(x^{1/2}\log^2 T\big) = \mathrm{O}\big(x^{1/2}\log^2 x\big).\end{aligned}$$

was die scharfe asymptotische Formel für $\psi(x)$ zeigt. Wir bemerken noch, daß diese ψ-Formel sogar äquivalent zur Riemannschen Vermutung ist, was ähnlich beweisbar ist.

Die Riemannsche Vermutung liefert also die gute Fehlerabschätzung der Größenordnung von etwa $x^{1/2}$, die man auch numerisch beobachtet. Man kann sagen, daß nach der Riemannschen Vermutung die Primzahlen so gleichmäßig wie nur möglich verteilt sind.

§ 1.2. Primzahlsätze in arithmetischen Progressionen und die allgemeine Riemannsche Vermutung

Dirichlet zeigte 1837, daß jede Restklasse $a \bmod q$, $(a,q) = 1$, („arithmetische Progression“ a, $a+q$, $a+2q, \ldots$, kurz „AP“) unendlich viele Primzahlen enthält.

Genauer läßt sich dies mit folgendem Satz formulieren, der mit den Methoden von Hadamard und de la Vallée–Poussin beweisbar ist:

Dirichletscher Primzahlsatz/Primzahlsatz in Progressionen: (DPZS)
Für $(a,q) = 1$ gilt

$$\psi(x;q,a) := \sum_{\substack{n\leq x\\ n\equiv a(q)}} \Lambda(n) = \frac{x}{\varphi(q)}\big(1+\mathrm{o}(1)\big)$$

und

$$\pi(x;q,a) := \#\big\{p \leq x : p \equiv a\ (q)\big\} = \frac{\operatorname{li}(x)}{\varphi(q)}\ \big(1+\mathrm{o}(1)\big).$$

Die von $\mathrm{o}(1)$ induzierten Funktionen können von q und a abhängen!
Noch genauer läßt sich $\pi(x;q,a) = \frac{\operatorname{li}(x)}{\varphi(q)} + \mathrm{O}\big(x\exp(-C(\log x)^{1/10})\big)$ zeigen, wobei die O–Konstante und C von a und q abhängen können; diese Formel ist sinnvoll für kleine q, wo der Fehlerterm von kleinerer Größenordnung ist als der Hauptterm.

Die Primzahlen verteilen sich nach dem DPZS asymptotisch gleichmäßig auf die $\varphi(q)$ vielen reduzierten Restklassen mod q.

Bemerkung. Eine Primzahl kann nur dann in einer *nicht*reduzierten Restklasse ad mod qd, $d \neq 1$, liegen, wenn $p = d$ und $a \equiv 1\ (q)$ ist. In einer nicht reduzierten Restklasse liegt also höchstens eine Primzahl.

In dieser Form ist der Dirichletsche Primzahlsatz eine einfache Verallgemeinerung des Primzahlsatzes. Da man in Anwendungen aber oft viele Restklassen gleichzeitig betrachten möchte, benötigt man aber eine Version des DPZS, die explizit in q und gleichmäßig in a ist. Eine solche Version ist der

Satz von Page: *Es gibt zu $C > 0$ eine positive Zahl $\delta > 0$, so daß für alle q mit $1 \leq q \leq e^{C\sqrt{\log x}}$, die nicht Vielfache einer natürlichen Zahl $q_1 = q_1(x)$ sind, und alle $(a, q) = 1$ gilt:*

$$\psi(x; q, a) = \frac{x}{\varphi(q)} + \mathrm{O}\big(x \exp(-\delta\sqrt{\log x})\big)$$

$$\textit{bzw.} \quad \pi(x; q, a) = \frac{\mathrm{li}(x)}{\varphi(q)} + \mathrm{O}\big(x \exp(-\delta\sqrt{\log x})\big),$$

wobei die O*–Konstante nur von δ abhängt.*
Die Ausnahmen für q machen diesen Satz allerdings etwas unhandlich. Ein weiteres Ergebnis zur Primzahlverteilung in Restklassen ist der wichtige

Satz von Siegel–Walfisz: *Für jedes (feste) $A > 0$ existiert eine Konstante $c_0 = c_0(A) > 0$, so daß für alle $q \leq (\log x)^A$ und $(a, q) = 1$ gilt:*

$$\pi(x; q, a) = \frac{\mathrm{li}(x)}{\varphi(x)} + \mathrm{O}\big(\exp(-c_0\sqrt{\log x})\big)$$

bzw.

$$\psi(x; q, a) = \frac{x}{\varphi(x)} + \mathrm{O}\big(\exp(-c_0\sqrt{\log x})\big)$$

(die O*–Konstante hängt dabei nur von A ab).*

Dieser Satz hat gegenüber dem von Page hingegen den Nachteil, daß er *ineffektiv* ist, d.h. die Konstante $c_0(A)$ und die O–Konstante können *nicht* effektiv in Abhängigkeit von A berechnet werden. Dies ist kein Mangel im Beweis, sondern ein prinzipielles Problem.

All diese Sätze über Primzahlen in arithmetischen Progessionen beweist man über die analytischen Eigenschaften von verallgemeinerten Riemannschen Zetafunktionen: Die **Dirichletschen L–funktionen**. Um diese zu definieren, benötigt man die sogenannten (Dirichlet–) **Charaktere** mod q, zu einer natürlichen Zahl q sind das Abbildungen $\chi : \mathbb{Z} \to \mathbb{C}$, die q–periodisch und vollständig multiplikativ sind mit der Eigenschaft, daß $\big|\chi(n)\big| = 1$ für $(n, q) = 1$ und $\chi(n) = 0$ für $(n, q) > 1$ gilt. Wir brauchen hier nicht weiter die Theorie dieser Charaktere zu vertiefen, da wir sie voraussichtlich nicht benötigen

werden. Zu solch einem Charakter $\chi \bmod q$ definiert man die zugehörige Dirichletsche L–funktion als

$$L(s,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1-\chi(p)p^{-s}} \quad \text{für } s \in \mathbb{C} \text{ mit } \operatorname{Re} s > 1.$$

Ebenso wie ζ läßt sich $L(s,\chi)$ holomorph auf $\mathbb{C}\backslash\{1\}$ fortsetzen, und wiederum mit einem einfachen Pol bei $s=1$. Wie ζ hat auch die L–Fortsetzung im kritischen Streifen $0 \le \operatorname{Re} s \le 1$ unendlich viele Nullstellen und deren (horizontale) Verteilung hat wichtige Implikationen über die Verteilung der Primzahlen in APs zur Folge.
Die oben angegebenen Primzahlsätze über Primzahlen in APs werden bewiesen, indem man zeigt, daß keine der betrachteten L–funktionen eine Nullstelle nahe der Geraden $\operatorname{Re} s = 1$ haben kann, und wie für ζ läßt sich auch für die L–funktionen die Riemannsche Vermutung formulieren:

Allgemeine Riemannsche Vermutung (GRH):
Sei $L(s,\chi)$ eine Dirichletsche L–funktion. Dann liegen alle Nullstellen von $L(s,\chi)$ mit $0 \le \operatorname{Re} s \le 1$ auf der Geraden $\operatorname{Re} s = \frac{1}{2}$.

Nimmt man die GRH an, so läßt sich für $q \le x, (a,q)=1$ wiederum schließen, daß

$$\pi(x;q,a) = \frac{\operatorname{li}(x)}{\varphi(q)} + \mathrm{O}(x^{1/2}\log x) \text{ unter (GRH)}$$
$$\text{bzw.} \quad \psi(x;q,a) = \frac{x}{\varphi(q)} + \mathrm{O}(x^{1/2}\log^2 x) \text{ unter (GRH)}$$

gilt, was für $1 \le q \le \frac{x^{1/2}}{(\log x)^{2+\varepsilon}}$ nichttrivial ist.

(Weil dann z. B. in der ψ-Formel der Hauptterm $\frac{x}{\varphi(q)} \ge \frac{x}{q} \ge x^{1/2}(\log x)^{2+\varepsilon}$ von größerer Größenordnung ist als der angegebene Fehlerterm $x^{1/2}\log^2 x$.)

In vielen Anwendungen braucht man nur, daß eine solche gute Fehler–Abschätzung lediglich „im Mittel“ über alle Moduln q gilt.
Man studiert daher die Differenz

$$\Delta(x;q,a) := \psi(x;q,a) - \frac{x}{\varphi(q)}$$

im Mittel über q, in dem man nach guten Abschätzungen für

$$E(x,Q) := \sum_{q \le Q} \max_{(a,q)=1} \max_{y \le x} \left|\Delta(y;q,a)\right|$$

sucht. Die triviale Schranke hierfür ist $E(x,Q) \ll x\log x$, da $\Delta(x;q,a) \ll \frac{x}{q}\log x$. Gefragt ist nun der größte Bereich für Q, für den eine nichttriviale Abschätzung für $E(x,Q)$

möglich ist. Das in dieser Hinsicht beste bekannte Ergebnis ist der

Satz von Bombieri–Vinogradov:
Für ein $A > 0$ existiert ein $B = B(A) > 0$ (etwa $B = A + 5/2$), so daß für alle $Q \leq x^{1/2}(\log x)^{-B}$ gilt:

$$E(x, Q) \ll x(\log x)^{-A}.$$

In vielen Fällen kann dieser Satz die Annahme der unbewiesenen Riemannschen Vermutung ersetzen.

§ 1.3. Exponentialsummen als Hilfsmittel

Für $\alpha \in \mathbb{R}$ definieren wir die (komplexe) Exponentialfunktion $e(\alpha) := \exp(2\pi i\alpha)$, welche offenbar 1–periodisch ist, und für eine Folge $(a_m) \subseteq \mathbb{C}$ definieren wir eine Exponentialsumme als $S(\alpha) := \sum\limits_{m \leq n} a_m\, e(\alpha m)$.

Warum so eine Summe wichtig für additive zahlentheoretische Probleme relevant sein kann, werden wir später noch genauer sehen. Dabei spielen folgende einfache Feststellungen eine wichtige Rolle:

1.) Die Exponentialfunktion $e(\alpha)$ erfüllt die **Orthogonalitätsrelation**

$$\int\limits_0^1 e(\alpha k)d\alpha = \begin{cases} 1, & k = 0 \\ 0, & k \in \mathbb{Z}\backslash\{0\}. \end{cases}$$

Beweis.

$$\int\limits_0^1 e(\alpha k)d\alpha = \int\limits_0^1 e^{2\pi i\alpha k}d\alpha = \begin{cases} \frac{1}{2\pi ik}\, e^{2\pi i\alpha k}\big|_0^1 = \frac{1}{2\pi ik}(1-1) = 0, & k \in \mathbb{Z}\backslash\{0\}, \\ \int\limits_0^1 1 d\alpha = 1, & k = 0. \end{cases}$$

□

2.) Sei $\|\alpha\| := \min\limits_{k\in\mathbb{Z}} |k - \alpha|$ der Abstand von α zur nächsten ganzen Zahl. Dann gilt für $M < N$, $M, N \in \mathbb{N}$, die Abschätzung

$$\Big|\sum_{M<n\leq N} e(\alpha n)\Big| \leq \min\Big\{N - M,\ \frac{1}{2\|\alpha\|}\Big\}$$

für den geometrischen Summenabschnitt $\sum\limits_{M<n\leq N} e(\alpha n)$.

Bemerkung. Ist $\alpha \in \mathbb{Z}$, also $\|\alpha\| = 0$, ist $\frac{1}{2\|\alpha\|} = \infty$ zu lesen und die rechte Seite ist dann $= N - M$.

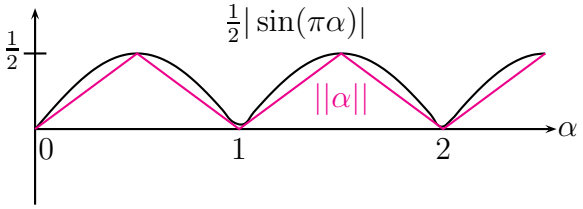
Beweis. Trivialerweise ist der Betrag der Summe stets $\leq N - M$. Andererseits ist er nach der Summenformel für geometrische Summen im Fall $\alpha \notin \mathbb{Z} \Leftrightarrow \|\alpha\| \neq 0$ dann

$$= \Big|e\big(\alpha(M+1)\big) \sum_{n=0}^{N-M-1} e(\alpha)^n\Big| = \Big|\frac{1 - e(\alpha(N-M))}{1 - e(\alpha)}\Big| \leq \frac{2}{\big|2 - 2\cos(2\pi\alpha)\big|^{1/2}}$$
$$= \frac{2}{2\big|\sin(\pi\alpha)\big|} \leq \frac{1}{2\|\alpha\|}.$$

Dabei wurde benutzt, daß

$$\big|1 - e^{2\pi i\alpha}\big|^2 = \big(1 - \cos(2\pi\alpha)\big)^2 + \sin^2(2\pi\alpha) = 2 - 2 \underbrace{\cos(2\pi\alpha)}_{\substack{\cos^2(\pi\alpha) - \sin^2(\pi\alpha) \\ = 1 - 2\sin^2(\pi\alpha)}} = 4\sin^2(\pi\alpha).$$

Zur letzten Ungleichung:



□

§ 2 Der Drei–Quadrate–Satz

Wir werden den folgenden Satz beweisen:

Satz 2.1. (Legendre/Gauß): *Für $n \in \mathbb{N}$ ist äquivalent:*

(1) n ist Summe dreier Quadrate, d.h. $n = x_1^2 + x_2^2 + x_3^2,\ x_i \in \mathbb{N}_0$, ist lösbar,

*(2) n ist **nicht** von der Form $4^a(8b+7)$ für $a, b \in \mathbb{N}_0$.*

In elementarer Zahlentheorie wurde die Richtung (1) $\Rightarrow$ (2) bewiesen, hier die Wiederholung:

Beweis. von (1) $\Rightarrow$ (2): Ann. Gelte (1) $\wedge \neg$ (2)

Sei ① $n = 4^a(8b+t),\ a, b \in \mathbb{N}_0$, und ② $n = x_1^2 + x_2^2 + x_3^2$
mit $x_j = 2^{a_j} y_j$, $2 \nmid y_j$, Œ $a_1 \leq a_2 \leq a_3$.

Beh. $a \overset{!}{=} a_1$
Ann. $a_1 > a$: Aus ② folgt dann $4^{a+1} | n$ im ↯ zur Gestalt $n = 4^a(8b+7)$ in ①.

Ann. $a_1 < a$: Mit ① folgt:

$$\underbrace{\frac{n}{4^{a_1}}}_{\substack{\equiv 0,4\ (8) \\ (\text{da } \equiv 0\ (4) \text{ für } a_1 < a_2)}} = 4^{a-a_1}(8b+7) = \underbrace{y_1^2}_{\equiv 1\ (8)} + \underbrace{2^{2(a_2-a_1)} y_2^2}_{\equiv 0,1,4\ (8)} + \underbrace{2^{2(a_3-a_1)} y_3^2}_{\equiv 0,1,4\ (8)}, \quad \text{↯}.$$

Es folgt

$$n_1 := \underbrace{8b+7}_{\equiv 7\ (8)} = \underbrace{\underbrace{y_1^2}_{\equiv 1\ (8)} + \underbrace{2^{b_2} y_2^2}_{\equiv 0,1,4\ (8)} + \underbrace{2^{b_3} y_3^2}_{\equiv 0,1,4\ (8)}}_{\text{aber: } \equiv 1,2,3,5,6\ (8)}, \text{ mit } 2 \nmid y_1, y_2, y_3,\ 0 \leq b_2 \leq b_3,$$

↯.

□

Da die Eigenschaft, Summe dreier □e zu sein, **nicht** multiplikativ ist (z.B. $3 \cdot 5 = (1^2 + 1^2 + 1^2) \cdot (2^2 + 1^2 + 0^2) = 15 = 4^0(8 \cdot 1 + 7)$ ist **nicht** $\sum$ 3er □e, s.o.), läßt sich (2) $\Rightarrow$ (1) nicht so beweisen wie der 2□e und 4□e –Satz. Wir benötigen dafür den Dirichletschen Primzahlsatz in arithmetischen Progressionen (s. §1) und einiges aus der Theorie der ternär–quadratischen Formen, was wir im nächsten Abschnitt entwickeln werden. Damit beweisen wir dann später Satz 2.1 zu Ende. Auch das QRG wird dabei eine zentrale Rolle spielen!

§ 2.1. Binär– und ternärquadratische Formen

1.) Sei $M_n(\mathbb{Z}) := \mathbb{Z}^{n\times n}$ der Ring der $n \times n$–Matrizen mit ganzzahligen Einträgen.

2.) $A \in M_n(\mathbb{Z})$ **symmetrisch** $:\Leftrightarrow A^T = A$, wo $A^T = (a_{ij}^T) = (a_{ji})$ für $A = (a_{ij})$ die transponierte Matrix bedeutet.

3.) $A, U \in M_n(\mathbb{Z})$, A symmetrisch $\Rightarrow$ U^TAU symmetrisch, da $(U^TAU)^T = U^TA^T(U^T)^T = U^TAU$.

4.) Sei $SL_n(\mathbb{Z})$ die Gruppe der $n \times n$–Matrizen mit ganzzahligen Einträgen und Determinante 1.

5.) $SL_n(\mathbb{Z})$ operiert auf $M_n(\mathbb{Z})$ vermöge: $SL_n(\mathbb{Z}) \times M_n(\mathbb{Z}) \to M_n(\mathbb{Z}) \rightsquigarrow A \cdot U := U^TAU$ (Notation von rechts)

$$\ulcorner \quad A \cdot (UV) = (UV)^TA(UV) = V^T(UAU)V = (U^TAU) \cdot V = (A \cdot U) \cdot V \quad \lrcorner$$

6.) $A, B \in M_n(\mathbb{Z})$ sind **äquivalent** $:\Leftrightarrow \exists\, U \in SL_n(\mathbb{Z}) : B = A \cdot U = U^TAU$
Notation: $A \sim B$ (Ü) $\sim$ ist eine Äquivalenzrelation.

7.) Für $U \in SL_n(\mathbb{Z})$ folgt

$$\det(A \cdot U) = \det(U^TAU) = \det(U^T)\det(A)\det(U) = \det(A),$$

d. h. die Gruppenop. erhält Determinanten. Weiter: A symmetrisch $\Rightarrow A \cdot U$ symmetrisch.

8.) Für $d \in \mathbb{Z}$ partitioniert die Gruppenop. die Menge der symmetrischen $n \times n$–Matrizen der Determinante d in Äquivalenz–Klassen.

9.) Zu $A = (a_{ij}) \in M_n(\mathbb{Z})$ symmetrisch definiert man die zugehörige **quadratische Form** F_A durch

$$F_A(x_1, \ldots, x_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij}\, x_i\, x_j,$$

ein homogenes Polynom vom Grad 2 in n Variablen $x_1, \ldots, x_n$.
Bsp. $F_{I_n}(x_1, \ldots, x_n) = x_1^2 + \cdots + x_n^2$.
Schreiben auch $x = (x_1, \ldots, x_n)^T$ und $F_A(x_1, \ldots, x_n) = F_A(x) = x^TAx$.

10.) $\operatorname{disc} F_A := \det A$ ist die **Diskriminante** von F_A.

11.) F_A **äquivalent** zu F_B, d. h. $F_A \sim F_B :\Leftrightarrow A \sim B$
Äquivalente Formen haben dieselbe Diskriminante.

12.) F_A **repräsentiert** $m \in \mathbb{Z}$, falls $m = F_A(x)$ für ein $x = (x_1, \ldots, x_n)$.
$A \sim B$, F_A repräsentiert $m \Rightarrow F_B$ repräsentiert m.
Also: Zwei äquivalente Formen repräsentieren exakt die gleiche Menge ganzer Zahlen, denn

$$A \sim B \Rightarrow A = U^T B U \Rightarrow m = F_A(x) = x^T A x = x^T U^T B U x = (Ux)^T B (Ux) = F_B(Ux).$$

Folgerung aus dem Satz von **Lagrange:** Für $n \geq 4$ repräsentiert jede quadratische Form äquivalent zu $x_1^2 + \cdots + x_n^2$ alle nichtnegativen ganzen Zahlen $\mathbb{N}_0$.

13.)

quadratische Form in 2 Variablen : binärquadratische Form
quadratische Form in 3 Variablen : ternärquadratische Form

14.) F_A **positiv definit**: $\Leftrightarrow \forall\, x \neq 0 : F_A(x) \geq 1$
Jede quadratische Form äquivalent zu einer positiv definiten Form ist positiv definit.

Ziel des §2.1: Für binär– und ternär- quadratische Formen gibt es genau eine Äquivalenzklasse **positiv–definiter** Formen der Diskriminante 1! (D.h. alle Formen sind äquivalent zu $x_1^2 + x_2^2$ bzw. $x_1^2 + x_2^2 + x_3^2$.)

Zunächst zum binärquadratischen Fall:

Lemma 2.2. *Zu $A \in \mathbb{Z}^{2\times 2}$ symmetrisch sei $F_A(x) = a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2$ die zugehörige quadratische Form. Dann gilt:*
F_A positiv–definit $\Leftrightarrow a_{11} \geq 1$ und $d := \det(A) = a_{11}a_{22} - a_{12}^2 \geq 1$.

[*vgl. Hurwitz-Kriterium*]

Beweis.

„ $\Rightarrow$ “ : $a_{11} = F_A(1,0) \geq 1$, $a_{11}\, d = a_{11}(a_{11}a_{22} - a_{12}^2) = a_{11}a_{12}^2 - 2a_{11}a_{12}^2 + a_{11}^2 a_{22}$
$= F_A(-a_{12}, a_{11}) \geq 1 \Rightarrow d \geq 1$.
„ $\Leftarrow$ “ : $a_{11} \geq 1$ & $d \geq 1 \Rightarrow a_{11}F_A(x_1,x_2) = (a_{11}x_1 + a_{12}x_2)^2 + dx_2^2 \geq 0$
und $F_A(x_1,x_2) = 0 \Leftrightarrow (x_1,x_2) = (0,0)$.

□

Lemma 2.3. *Jede Äquivalenz–Klasse positiv–definiter binärquadratischer Formen der Diskriminante d enthält (mindestens) eine Form $F_A(x_1,x_2) = a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2$ mit $2\,|a_{12}| \leq a_{11} \leq \frac{2}{\sqrt{3}}\sqrt{d}$.*

Beweis. Betr. F_B, positiv–definit, zur Matrix $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{12} & b_{22} \end{pmatrix}$.
Sei $a_{11} := \min\{n > 0; \exists\, x_1, x_2 : n = F_B(x_1, x_2)\}$, etwa $a_{11} = F_B(r_1, r_2)$.
Dabei ist $(r_1, r_2) = 1$.
$\ulcorner$ Sonst : $1 < h \mid (r_1, r_2) \Rightarrow a_{11} \leq F_B\left(\frac{r_1}{h}, \frac{r_2}{h}\right) = \frac{F_B(r_1,r_2)}{h^2} = \frac{a_{11}}{h^2} < a_{11}, \lightning$. $\lrcorner$

Sei $1 = r_1 s_2 - r_1 s_1 = r_1(s_2 + r_2 t) - r_2(s_1 + r_1 t)$ für alle $t \in \mathbb{Z}$.
$\Rightarrow \forall\, t \in \mathbb{Z} : U := \begin{pmatrix} r_1 & s_1 + r_1 t \\ r_2 & s_2 + r_2 t \end{pmatrix} \in SL_2(\mathbb{Z})$.
Setze $A := U^T B U = \begin{pmatrix} F(r_1, r_2) & a'_{12} + F(r_1, r_2)t \\ a'_{12} + F(r_1, r_2)t & F(s_1 + r_1 t, s_2 + r_2 t) \end{pmatrix} \rightsquigarrow a_{11}, a_{12}, a_{22}$
mit $a'_{12} = b_{11} r_1 s_1 + b_{12}(r_1 s_2 + r_2 s_1) + b_{22} r_2 s_2$, und $a_{22} \geq a_{11}$ da $(s_1 + r_1 t, s_2 + r_2 t) \neq (0, 0)$ für alle $t \in \mathbb{Z}$.

Nun wähle t so, dass $|a_{12}| = |a'_{12} + a_{11} t| \leq \frac{a_{11}}{2}$. ($\rightsquigarrow$ 1. Ungl. $\checkmark$)
Also $A \sim B$ mit $2|a_{12}| \leq a_{22}$. Sei $d := a_{11} a_{22} - a_{12}^2$ die Diskriminante.
Mit $a_{11}^2 \leq a_{11} a_{22} = d + a_{12}^2 \leq d + \frac{a_{11}^2}{4}$ folgt $\frac{3 a_{11}^2}{4} \leq d \Leftrightarrow a_{11} \leq \frac{2}{\sqrt{3}} \cdot \sqrt{d}$.
($\rightsquigarrow$ 2. Ungl. $\checkmark$) $\square$

Bemerkung. Für diese binärquadratische Form F_A ist also
$a_{11} = \min\{n = F_B(x_1, x_2) \neq 0\}$.

Satz 2.4. *Jede positiv–definite binärquadratische Form der Diskriminante* 1 *ist äquivalent zu* $x_1^2 + x_2^2$.

Beweis. Sei F so. Aus Lemma 2.3 folgt $F \sim a_{11} x_1^2 + 2 a_{12} x_1 x_2 + a_{22} x_2^2$ mit $2|a_{12}| \leq a_{11} \leq \frac{2}{\sqrt{3}} < 2$. Da $a_{11} \geq 1$ (Lemma 2.2), folgt $a_{11} = 1$, also $a_{12} = 0$.
Da $1 = a_{11} a_{22} - a_{12}^2 = a_{22}$, ist also $F \sim x_1^2 + x_2^2$. $\square$

Nun zu ternärquadratischen Formen:

Lemma 2.5. *Sei* $A \in \mathbb{Z}^{3\times 3}$ *symmetrisch,* F_A *die zugehörige ternärquadratische Form,* $d = \operatorname{disc} F_A$. *Dann gilt:*

(1) $a_{11} F_A(x) = (a_{11} x_1 + a_{12} x_2 + a_{13} x_3)^2 + G_{A^*}(x_2, x_3)$ *mit der binärquadratischen Form* G_{A^*} *zur Matrix* $A^* = \begin{pmatrix} a_{11} a_{22} - a_{12}^2 & a_{11} a_{23} - a_{12} a_{13} \\ a_{11} a_{23} - a_{12} a_{13} & a_{11} a_{33} - a_{13}^2 \end{pmatrix}$ *mit* $\operatorname{disc} G_{A^*} = \det A^* = a_{11} d$.

(2) Es gilt: F_A *positiv definit* $\Rightarrow$ G_{A^*} *positiv definit.*

(3) Weiter: F_A positiv definit $\Leftrightarrow$ $\begin{cases} a_{11} = \det(a_{11}) \geq 1 \\ d' = \det \begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix} \geq 1 \\ d = \det(A) \geq 1. \end{cases}$

Beweis. Obige Beh. (1) zeigt man durch Rechnen... (Ü)

Zu (2) und (3)„⇒ “: Ist F_A positiv definit, ist $a_{11} = F_A(1,0,0) \geq 1$.
Ist $G_{A^*}(x_2, x_3) \leq 0$ für $x_2, x_3 \in \mathbb{Z}$, folgt $G_{A^*}(a_{11}x_2, a_{11}x_3) = a_{11}^2 G_{A^*}(x_2, x_3) \leq 0$.
Sei $x_1 := -(a_{12}x_2 + a_{13}x_3)$, d.h. $a_{11}x_1 + a_{12}a_{11}x_2 + a_{13}a_{11}x_3 = 0$ und

$$\underbrace{a_{11}}_{\geq 1} \cdot \underbrace{F_A(x_1, a_{11}x_2, a_{11}x_3)}_{\text{positiv definit}} = 0^2 + G_{A^*}(a_{11}x_2, a_{11}x_3) \leq 0 \Rightarrow x_2 = x_3 = 0.$$

Dies zeigt: G_{A^*} ist auch positiv definit.
Mit Lemma 2.2 folgt: Der Leitkoeffizient von G_{A^*} ist > 0, d. h. $d' = a_{11}a_{22} - a_{12}^2 \geq 1$.
Weiter ist $\operatorname{disc} G_{A^*} = \underbrace{\det A^*}_{=a_{11}d} \geq 1$ nach Lemma 2.2, also ist $d = \det(A) \geq 1$.

Zu (3)„⇐ “: Lemma 2.2 zeigt, daß G_{A^*} positiv definit ist. Klar: $F_A(x) \geq 0$ für alle $x = (x_1, x_2, x_3)^T$.
Ist $F_A(x_1, x_2, x_3) = 0$, folgt also aus (1), daß

$$\underbrace{G_{A^*}(x_2, x_3) = 0}_{\Rightarrow x_2 = x_3 = 0, \text{ da } G_{A^*} \text{ pos. def.}} \quad \& \underbrace{a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = 0}_{\Rightarrow\ x_1 = 0}.$$

Also ist F_A positiv definit. □

Bem. (1) liefert zu einer ternärquadratischen Form F_A eindeutig eine binärquadratische Form G_{A^*}. Nun gilt: Eine bestimmte Menge ternärquadratischer Formen $F_{A_{r,s}}$ in einer Äquivalenz–Klasse $\sim F_B$ hat dieselbe zugehörige binärquadratische Form G_{A^*}, wie folgendes Lemma zeigt.

Lemma 2.6. *Sei $B = (b_{ij}) \in \mathbb{Z}^{3\times 3}$ symmetrisch, F_B positiv definit.*
Sei G_{B^*} die eindeutig positiv definite binärquadratische Form mit

$$b_{11}\, F_B(y) = (b_{11}y_1 + b_{12}y_2 + b_{13}y_3)^2 + G_{B^*}(y_2, y_3) \text{ gemäß Lemma 2.5.}$$

Für $V^* = (v_{ij}^*) \in SL_2(\mathbb{Z})$ setze $A^* := (V^*)^T B^* V^*$ und G_{A^*} als zugehörige positiv definite binärquadratische Form zu A^*, äquivalent zu G_{B^*}. (✓)
Für $r, s \in \mathbb{Z}$ setze

$$V_{r,s} = (v_{ij}) := \begin{pmatrix} 1 & r & s \\ 0 & v_{11}^* & v_{12}^* \\ 0 & v_{21}^* & v_{22}^* \end{pmatrix} \in SL_3(\mathbb{Z})$$

und $A_{r,s} = V_{r,s}^T\, B\, V_{r,s} =: (a_{ij})$ *(abh. von* r, s*) mit zugehöriger ternärquadratischer Form* $F_{A_{r,s}}$.
Dann gilt: $a_{11} = b_{11}$ *und* $a_{11}\, F_{A_{r,s}}(x) = (a_{11}x_1 + a_{12}x_2 + a_{13}x_3)^2 + G_{A^*}(x_2, x_3)$ *mit obiger Matrix* A^**, die ja unabhängig von* r *und* s *ist (ebenso* $a_{11} = b_{11}$*).*
D.h. $G^*_{A_{r,s}} = G_{A^*}$*, alle* $F_{A_{r,s}} \sim F_B$.

Beweis. Haben $v_{11} = 1,\ v_{21} = v_{31} = 0$, also ist wegen

$$A_{r,s} = V_{r,s}^T B V_{r,s} \text{ dann } a_{1_j} = \sum_{k=1}^{3}\sum_{i=1}^{3} v_{1k}^T\, b_{ki} v_{ij} = \sum_{k=1}^{3}\sum_{i=1}^{3} v_{k1} b_{ki} v_{ij} = \sum_{i=1}^{3} b_{1i} v_{ij},$$

also $a_{11} = b_{11}$. ✓
Sei $x = (x_1, x_2, x_3)^T,\ V_{r,s}x =: y = (y_1, y_2, y_3)^T$ also $y_i = \sum\limits_{j=1}^{3} v_{ij}x_j$.
Insbesondere:

$$\begin{aligned} y_2 &= \overbrace{v_{21}x_1}^{=0} + v_{22}x_2 + v_{23}x_3 = v_{11}^* x_2 + v_{12}^* x_3, \\ y_3 &= \underbrace{v_{31}x_1}_{=0} + v_{32}x_2 + v_{33}x_3 = v_{21}^* x_2 + v_{22}^* x_3. \end{aligned}$$

Mit $y^* := \begin{pmatrix} y_2 \\ y_3 \end{pmatrix}$ und $x^* := \begin{pmatrix} x_2 \\ x_3 \end{pmatrix}$ ist also $V^* x^* = y^*$
Es folgt: $G_{B^*}(y^*) = G_{B^*}(V^* v^*) = G_{A^*}(x^*)$
und

$$b_{11}y_1 + b_{12}y_2 + b_{13}y_3 = \sum_{i=1}^{3} b_{1i} \sum_{j=1}^{3} v_{ij}x_j = \sum_{j=1}^{3} \underbrace{\Big(\sum_{i=1}^{3} b_{1i}v_{ij}\Big)}_{=a_{1j}} x_j.$$

Da

$$\begin{aligned} &F_{A_{r,s}}(x) = x^T A_{r,s} x = (V_{r,s}x)^T B (V_{r,s}x) = y^T B y = F_B(y) \text{ ist, folgt} \\ &(a_{11}x_1 + a_{12}x_2 + a_{13}x_3)^2 + G_{A^*_{r,s}}(x_2, x_3) = a_{11} F_{A_{r,s}}(x) = b_{11} F_B(y) \\ &\quad = (b_{11}y_1 + b_{12}y_2 + b_{13}y_3)^2 + G_{B^*}(y_2, y_3) = (a_{11}x_1 + a_{12}x_2 + a_{13}x_3)^2 + G_{A^*}(x_2, x_3), \end{aligned}$$

also ist $G_{A^*_{r,s}}(x_2, x_3) = G_{A^*}(x_2, x_3)$ für alle $x_2, x_3 \in \mathbb{Z}$. □

Lemma 2.7. *Seien* $u_{11}, u_{21}, u_{31} \in \mathbb{Z},\ (u_{11}, u_{21}, u_{31}) = 1$.
Dann existieren 6 *ganze Zahlen* $u_{ij},\ i = 1, 2, 3,\ j = 2, 3$*, so daß* $U = (u_{ij}) \in SL_3(\mathbb{Z})$*, d. h.* $\det U = 1$.

Beweis. Sei $a := (u_{11}, u_{21})$, wähle u_{12}, u_{22} mit $u_{11}u_{22} - u_{21}u_{12} = a$
(Darstellung des ggT mit Euklidischen Algorithmus).
Da $(a, u_{31}) = (u_{11}, u_{21}, u_{31}) = 1$, wähle u_{33}, b mit $au_{33} - bu_{31} = 1$ (ebenso).

Sei $u_{13} := \underbrace{\frac{u_{11}b}{a}}_{\in\mathbb{Z},\text{ da } a|u_{11}}$, $u_{23} := \underbrace{\frac{u_{21}b}{a}}_{\in\mathbb{Z},\text{ da } a|u_{21}}$, $u_{32} := 0$. Dann: $U = (u_{ij}) \in \mathbb{Z}^{3\times 3}$ mit $\det U = 1$.
(Nachrechnen und Entwickeln nach letzter Spalte.) □

Lemma 2.8. *Jede Äquivalenzklasse positiv definiter ternärquadratischer Formen der Diskriminante d enthält (mindestens) eine Form $\sum_{i,j=1}^{3} a_{ij}x_ix_j$ mit*
$2\max\big(|a_{12}|, |a_{13}|\big) \le a_{11} \le \frac{4}{3}\cdot\sqrt[3]{d}$.

Beweis. Sei F positiv definite ternärquadratische Form mit $\operatorname{disc} F = d$, und $C \in \mathbb{Z}^{3\times 3}$ die zugehörige symmetrische Matrix.
Sei $a_{11} := \min\big\{F(x); x \neq 0\big\}$ und $a_{11} = F(u_{11}, u_{21}, u_{31})$.
Dann ist $(u_{11}, u_{21}, u_{31}) = 1$.
⌜ **Sonst**: $(u_{11}, u_{21}, u_{31}) =: h > 1 \;\Rightarrow\; F\big(\frac{u_{11}}{h}, \frac{u_{21}}{h}, \frac{u_{31}}{h}\big) = \frac{a_{11}}{h^2} < a_{11}$,
im ↯ zur Minimalität von a_{11}. ⌟

Wegen Lemma 2.7 existieren $u_{ij}, i = 1, 2, 3,\ j = 2, 3$ mit $U = (u_{ij}) \in SL_3(\mathbb{Z})$.
Sei $B := U^TCU = (b_{ij})$.
Also: $F \sim F_B$, und $b_{11} = a_{11}$ ist ebenso die kleinste Zahl $\neq 0$, die von F_B dargestellt wird.
(Äquivalente Formen repräsentieren die gleiche Zahlenmenge, s. Punkt 12.) oben.)

Mit Lemma 2.5 folgt
$a_{11}F_B(x) = (b_{11}x_1 + b_{12}x_2 + b_{13}x_3)^2 + \underbrace{G_{B^*}(x_2, x_3)}_{\text{positiv definit mit Diskriminante } a_{11}d}$

Mit Lemma 2.3 folgt $G_{B^*}(x_2, x_3) \sim G_{A^*}(x_2, x_3) = a_{11}^*x_2^2 + 2a_{12}^*x_2x_3 + a_{22}^*x_3^2$ mit $a_{11}^* \le \frac{2}{\sqrt{3}}\sqrt{a_{11}d}$.

Sei $V^* \in SL_2(\mathbb{Z})$ mit $A^* = (V^*)^TB^*V^*$.
Seien $r, s \in \mathbb{Z}$ und $V_{r,s} \in SL_3(\mathbb{Z})$ definiert wie in Lemma 2.6. Sei $A := V_{r,s}^T\, B\, V_{r,s} =: (a_{ij})$.

Mit Lemma 2.5 folgt
$a_{11}^* = a_{11}a_{22} - a_{12}^2$.

$$\overset{\text{Definition von } A}{\Rightarrow} \qquad \begin{cases} a_{12} = a_{11}r + b_{12}v_{11}^* + b_{13}v_{21}^* \\ a_{13} = a_{11}s + b_{12}v_{12}^* + b_{13}v_{22}^*. \end{cases}$$

$\rightsquigarrow$ Wähle r so, daß $|a_{12}| < \frac{a_{11}}{2}$, und s so, daß $|a_{13}| \leq \frac{a_{11}}{2}$. (1. Unglg. der Beh. ✓)

Da $a_{11} \leq F_A(0,1,0) = a_{22}$ (Minimalität von a_{11}), folgt
$a_{11}^2 \leq a_{11}a_{22} = a_{11}a_{22} - a_{12}^2 + a_{12}^2 = a_{11}^* + a_{12}^2 \leq \frac{2}{\sqrt{3}}\sqrt{a_{11}d} + \frac{a_{11}^2}{4}$
$\Rightarrow a_{11}^2 \leq \left(\frac{2}{\sqrt{3}}\right)^3 \sqrt{a_{11}d} \Rightarrow a_{11} \leq \frac{4}{3}\sqrt[3]{d}$ (2. Unglg. ✓) □

Satz 2.9. *Jede positiv definite ternärquadratische Form der Diskriminante* 1 *ist äquivalent zu* $x_1^2 + x_2^2 + x_3^2$.

Beweis. Sei F so. Nach Lemma 2.8 ist F äquivalent zu $F_A = \sum_{i,j=1}^{3} a_{ij}x_ix_j$, $\det A = 1$, mit $0 \leq 2\max\left(|a_{12}|, |a_{13}|\right) \leq a_{11} \leq \frac{4}{3}$.
Es folgt $a_{12} = a_{13} = 0$. Da $d \neq 0$, folgt $a_{11} \neq 0$, also $a_{11} = 1$.

Somit: $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & & \\ 0 & & A^* \end{pmatrix}$ mit $A^* = \begin{pmatrix} a_{22} & a_{23} \\ a_{23} & a_{33} \end{pmatrix}$, wo $\det A^* = 1$.

Nach Satz 2.4 ex. $U^* = \begin{pmatrix} u_{22} & u_{23} \\ u_{32} & a_{33} \end{pmatrix} \in SL_2(\mathbb{Z}) : (U^*)^T A^* U = I_2$.

Sei $U := \begin{pmatrix} 1 & 0 & 0 \\ 0 & & \\ 0 & & U^* \end{pmatrix}$, dann ist $U^T AU = I_3$, also $F \sim x_1^2 + x_2^2 + x_3^2$. □

§ 2.2. Summen von 3 Quadraten

Lemma 2.10. *Sei* $n \geq 2$ *und* $d' \in \mathbb{N}$, *so dass* $-d'$ *quadratischer Rest mod* $d'n - 1$ *ist. Dann ist* n *Summe von* 3 *Quadraten.*

Beweis. Es existieren $a_{12}, a_{11} \in \mathbb{Z}$ mit $a_{12}^2 + d' = a_{11}(d'n - 1) = a_{11}a_{22}$,
wo $a_{22} := d'n - 1 \geq 2d' - 1 \geq 1$, also ist $a_{11} \geq 1$.
Nun: $d' = a_{11}a_{22} - a_{12}^2$. Die Matrix $A = \begin{pmatrix} a_{11} & a_{12} & 1 \\ a_{12} & a_{22} & 0 \\ 1 & 0 & n \end{pmatrix}$
hat die Determinante $\det(A) = (a_{11}a_{22} - a_{12}^2)n - a_{22} = d'n - a_{22} = 1$.
Aus Lemma 2.5 folgt, daß F_A (zur Matrix A) positiv definit ist. Ferner ist $\operatorname{disc} F_A = \det(A) = 1$ und $n = F_A(0,0,1)$. Mit Satz 2.9 folgt, daß auch $x_1^2 + x_2^2 + x_3^2$ die Zahl n repräsentiert. □

Lemma 2.11. $n \in \mathbb{N}$, $n \equiv 2\ (4) \Rightarrow n$ *ist Summe von* 3 *Quadraten.*

Beweis. Da $(4n, n-1) = 1$, enthält die arithmetische Progression $\{4nj + n - 1;\ j = 1, 2, \dots\}$ unendlich viele Primzahlen. (Nach dem **Dirichletschen Primzahlsatz**, vgl. §

1).
Sei $j \geq 1$ so, daß $p = 4nj + n - 1 = (4j+1)n - 1$ prim.
Setze $d' := 4j+1 \Rightarrow p = \underbrace{d'n}_{\equiv 2\ (4)} - 1 \equiv 1\ (4)$, da $n \equiv 2\ (4)$.
Wegen Lemma 2.10 genügt es, z. z.: $-d'$ ist quadratischer Rest mod p. Sei $d' = \prod_i q_i^{k_i}$ die PFZ von d'. Dann: $p = d'n - 1 \equiv -1\ (qi)$ für alle i, und $1 \equiv d' \equiv \prod_{i,\ q_i \equiv 3\ (4)} (-1)^{k_i}\ (4)$, also ist $\prod_{i,\ q_i \equiv 3\ (4)} (-1)^{k_i} = 1$.

$\overset{\text{1.EG des QRG}}{\Rightarrow}$ $\left(\frac{-1}{p}\right) = 1$, da $p \equiv 1\ (4)$, und:

$$\left(\frac{-d'}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d'}{p}\right) = \prod_i \left(\frac{q_i}{p}\right)^{k_i} \overset{\text{QRG}}{=} \prod_i \left(\frac{p}{q_i}\right)^{k_i}$$
$$\overset{p \equiv -1\ (q_i)}{=} \prod_i \left(\frac{-1}{q_i}\right)^{k_i} = \prod_{i,\ q_i \equiv 3\ (4)} (-1)^{k_i} = 1.$$

□

Lemma 2.12. *$n \in \mathbb{N}, n \equiv 1,3,5\ (8) \Rightarrow n$ ist Summe von 3 Quadraten.*

Beweis. Klar: $n = 1$ ist Summe von 3 Quadraten. Sei also $n \geq 2$,

und $c := \begin{cases} 3, & n \equiv 1\ (8) \\ 1, & n \equiv 3\ (8) \\ 3, & n \equiv 5\ (8) \end{cases}$

Für $n \equiv 1,3\ (8)$ ist $\frac{cn-1}{2} \equiv 1\ (4)$, für $n \equiv 5\ (8)$ ist $\frac{cn-1}{2} \equiv 3\ (4)$.

Jedenfalls: $\left(4n, \frac{cn-1}{2}\right) = 1$.
$\ulcorner \left(4n, \frac{cn-1}{2}\right) = d \Rightarrow d \mid n$ & $d \mid cn - 1$, da $\frac{cn-1}{2}$ ungerade, also ist $d \mid 1$, also $d = 1$. $\lrcorner$

Nach dem **Dirichletschen Primzahlsatz** existiert eine Primzahl p der Form $p = 4nj + \frac{cn-1}{2}$ für ein $j \in \mathbb{N}$. Sei $d' := 8j + c$.
Dann: $2p = (8j+c)n - 1 = d'n - 1$.
Wegen Lemma 2.10 genügt, z. z.: $-d'$ ist quadratischer Rest mod $2p$. Weiter genügt, z. z.: $-d'$ ist quadratischer Rest mod p.
$\ulcorner$ Denn ist $-d'$ quadratischer Rest mod p, so existiert ein $x_0 \in \mathbb{Z}$ mit $(x_0 + p)^2 + d' \equiv x_0^2 + d' \equiv 0\ (p)$.
Sei $x := \left\{ \begin{array}{ll} x_0, & 2 \nmid x_0 \\ x_0 + p, & 2 \mid x_0 \end{array} \right\}$, dann ist $2 \nmid x$ und $x^2 + d'^2 \equiv 0\ (2)$. Also: $x^2 + d' \equiv 0\ (2p)$, und dann ist $-d'$ ein quadratischer Rest mod $2p$. $\lrcorner$

Sei nun $d' = \prod_i q_i^{k_1}$ die PFZ von d'.
Da $2p \equiv -1\ (d')$ folgt $2p \equiv -1\ (q_i)$ und $(p_i, q_i) = 1$ für alle i.

- Ist $n \equiv 1,3\ (8)$, folgt $p \equiv 1\ (4)$ und
  $\left(\frac{-d'}{p}\right) = \underbrace{\left(\frac{-1}{p}\right)}_{=1,\ 1.\ \text{EG}} \left(\frac{d'}{p}\right) = \left(\frac{d'}{p}\right) = \prod_i \left(\frac{q_i}{p}\right)^{k_i} = \prod_i \left(\frac{p}{q_i}\right)^{k_i}$.

- Ist $n \equiv 5\ (8)$, folgt $p \equiv 3\ (4)$ und $d' \equiv 3\ (8)$. Dann ist

  $$-1 \equiv d' = \prod_{i,\ q_i \equiv 1\ (4)} q_i^{k_i} \cdot \prod_{i,\ q_i \equiv 3\ (4)} q_i^{k_i} \equiv \prod_{i,\ q_i \equiv 3\ (4)} (-1)^{k_i}\ (4), \text{ also } \prod_{i,\ q_i \equiv 3\ (4)} (-1)^{k_i} = -1.$$

  Mit dem QRG folgt dann:

  $$\begin{aligned}\left(\frac{-d'}{p}\right) &= \left(\frac{-1}{p}\right) \cdot \left(\frac{d'}{p}\right) = -\left(\frac{d'}{p}\right) = -\prod_{i,\ q_i \equiv 1\ (4)} \left(\frac{q_i}{p}\right)^{k_i} \cdot \prod_{i,\ q_i \equiv 3\ (4)} \left(\frac{q_i}{p}\right)^{k_i} \\ &= -\prod_{i,\ q_i \equiv 1\ (4)} \left(\frac{p}{q_i}\right)^{k} \cdot \prod_{i,\ q_i \equiv 3\ (4)} \left(\frac{p}{q_i}\right)^{k} \underbrace{\prod_{i,\ q_i \equiv 3\ (4)} (-1)^{k}}_{=-1} \\ &= \prod_i \left(\frac{p}{q_i}\right)^{k_i}.\end{aligned}$$

- In beiden Fällen:

  $$\begin{aligned}\left(\frac{-d'}{p}\right) = \prod_i \left(\frac{p}{q_i}\right)^{k_i} = \prod_i \left(\frac{2}{q_i}\right)^{k_i} \cdot \left(\frac{2p}{q_i}\right)^{k_i} = \prod_i \left(\frac{2}{q_i}\right)^{k_i} \left(\frac{-1}{q_i}\right)^{k_i} \\ \overset{1.\&2.\ \text{EG}}{=} \underbrace{\prod_{i,\ q_i \equiv 3,5\ (8)} (-1)^{k_i}}_{\text{da } \equiv \pm 3\ (8)} \cdot \underbrace{\prod_{i,\ q_i \equiv 3,7\ (8)} (-1)^{k_i}}_{\text{da } \equiv 3\ (4)} = \prod_{i,\ q_i \equiv 5,7\ (8)} (-1)^{k_i}.\end{aligned}$$

  Somit ist $-d'$ quadratischer Rest mod p, falls $\sum_{i,\ q_i \equiv 5,7\ (8)} k_i \equiv 0\ (2)$.

  Dies zeigen wir nun:

  $$\begin{aligned}d' &= \underbrace{\prod_{i,\ q_i \equiv 1\ (8)} q_i^{k_i}}_{\equiv 1\ (8)} \cdot \prod_{i,\ q_i \equiv 3\ (8)} q_i^{k_i} \cdot \prod_{i,\ q_i \equiv 5\ (8)} q_i^{k_i} \cdot \prod_{i,\ q_i \equiv 7\ (8)} q_i^{k_i} \\ &\equiv \prod_{i,\ q_i \equiv 3\ (8)} 3^{k_i} \cdot \prod_{i,\ q_i \equiv 5\ (8)} (-3)^{k_i} \prod_{i,\ q_i \equiv 7\ (8)} (-1)^{k_i}\ (\text{mod } 8) \\ &\equiv \prod_{i,\ q_i \equiv 3,5\ (8)} 3^{k_i} \cdot \prod_{i,\ q_i \equiv 5,7\ (8)} (-1)^{k_i}\ (\text{mod } 8) \\ &\equiv 3^{\sum_{i,\ q_i \equiv 3,5\ (8)} k_i} \cdot (-1)^{\sum_{i,\ q_i \equiv 5,7\ (8)} k_i}\ (\text{mod } 8).\end{aligned}$$

- Für $n \equiv 1,5\ (8)$ ist $c = 3$ und $d' = 8_j + 3 \equiv 3\ (8)$,
  also $\sum_{i,\ q_i \equiv 3,5\ (8)} k_i \equiv 1\ (2)$, $\sum_{i,\ q_i \equiv 5,7\ (8)} k_i \equiv 0\ (2)$. ✓
- Für $n \equiv 3\ (8)$ ist $c = 1$ und $d' = 8j + 1 \equiv 1\ (8)$,
  also $\sum_{i,\ q_i \equiv 3,5\ (8)} k_i \equiv 0\ (2)$, $\sum_{i,\ q_i \equiv 5,7\ (8)} k_i \equiv 0\ (2)$. ✓

□

Nun sind wir in der Lage, Satz 2.1, (2) ⇒ (1), zu Ende zu beweisen, d. h. wir zeigen nun: Ist n **nicht** von der Form $n = 4^a(8b + 7), a, b \in \mathbb{N}_0$, so läßt sich n als Summe von 3 Quadraten schreiben.

Beweis. von (2) ⇒ (1): Schreibe $n = 4^a m$, wo $m \equiv 2\ (4)$ oder $m \equiv 1, 3, 5\ (8)$. Lemma 2.11 und Lemma 2.12 zeigen, daß sich m als Summe von 3 □en schreiben läßt, und damit auch $n = 4^a m$, da 4^a für $a \geq 0$ ein □ ist. □

□□□

Satz 2.13. (Zusatz) *Ist $n \equiv 3\ (8)$, läßt sich n als Summe von 3 ungeraden □en schreiben.*

Beweis. Mit Satz (2.1) ist $n = \underbrace{x_1^2}_{\equiv 0,1,4\ (8)} + \underbrace{x_2^2}_{\equiv 0,1,4\ (8)} + \underbrace{x_3^2}_{\equiv 0,1,4\ (8)} \equiv 3\ (8)$, dies ist nur möglich, wenn $x_1^2, x_2^2, x_3^2 \equiv 1\ (8)$, d. h. wenn x_1^2, x_2^2, x_3^2 ungerade □e sind. □

Im nächsten § bringen wir eine Anwendung des 3–Quadrate–Satzes.

§ 2.3. Dünne Mengen von Quadraten

Sei $A \subseteq \mathbb{N}_0$ eine endliche Menge.
Definition: A **Basis bezüglich** h **für** $n :\Leftrightarrow$
$\forall\, m \in \{0, 1, \ldots, n\}\, \exists\, a_1, \ldots, a_h \in A : m = a_1 + \cdots + a_h$.
D. h. jedes $m \leq n$ läßt sich als Summe von h vielen Elementen von A schreiben, wobei Wiederholungen erlaubt sind. Wir zeigen zunächst mit einem „Abzählargument“: Ist A eine Basis bezüglich h für n, kann A nicht **zu** klein sein.

Satz 2.14. *Sei $h \geq 2$. Es gibt eine Konstante $c = c(h) > 0$ so, dass gilt: Ist A eine Basis bezüglich h für n, so ist $\#A > c\, n^{1/h}$.*

Beweis. Sei $k := \#A$. Jedes $m \in \{0, 1, \ldots, n\}$ ist Summe von h vielen Elementen von A, mit Wiederholung. **Kombinatorik** ⇝ Die Anzahl der Kombinationen von h vielen Elementen mit Wiederholung einer Menge mit k Elementen ist $\binom{k+h-1}{h}$.

Somit ist

$$n+1 \le \binom{k+h-1}{h} = \frac{k(k+1)\cdots(k+h-1)}{h!} \le \frac{c'k^h}{h!}$$

für $c' := h^h > 0$ und alle k, $[k+h-1 \le k\cdot h\ \checkmark]$,
also ist

$$\#A = k > \Big(\frac{h!n}{c'}\Big)^{1/h} = c\,n^{1/h} \text{ mit } c = c(h) := \Big(\frac{h!}{c'}\Big)^{1/h} > 0.$$

□

Lagrange $\rightsquigarrow$ Die Menge $Q_n := \{k^2 \le n\}$ der Quadrate $\le n$
ist eine Basis bezüglich 4 für n. ✓
Und: $\#\,Q_n = 1 + \lfloor n^{1/2}\rfloor > n^{1/2}$, was $\gg c\,n^{1/4}$, nach Satz 2.14 die kleinstmögliche Anzahl einer Basis bezüglich 4.
Frage: Gibt es für jedes n eine dünnere Menge A_n aus Quadraten, die Basis bezüglich 4 für n ist, d. h. mit $\lim\limits_{n\to\infty} \frac{A_n}{n^{1/2}} = 0$?
Dies beantwortet:

Satz 2.15. (Choi–Erdős–Nathanson) *Für alle $n \ge 2$ existiert eine Menge A_n aus Quadraten so, daß A_n eine Basis bezüglich 4 für n ist, und daß $\#\,A_n \le \big(\frac{4}{\log 2}\big)\cdot n^{1/3}\log n$ gilt.*

Beweis. Die Mengen $A_2 = A_3 := \{0,1\},\ A_4 = A_5 := \{0,1,4\}$, erfüllen die Behauptung, also sei $\mathfrak{O}\, n \ge 6$.
Wir bemerken:

$$(*)\begin{cases} \text{ist } m \not\equiv 0\ (4) \text{ und } a^2 \le m, \\ \text{so ist } \underbrace{m}_{\equiv 1,2,3} - \underbrace{a^2}_{\equiv 0,1\ (4)} \text{ oder } \underbrace{m}_{\equiv 1,2,3} - \underbrace{(a-1)^2}_{\equiv 1,0\ (4)} \text{ kongruent zu } 1,2\ (4) \\ \text{und damit Summe von 3 } \square\text{en nach Satz 2.1.} \end{cases}$$

Für $n \ge 6$ sei $A_n^{(1)} := \{\ell^2;\ 0 \le \ell \le 2\,n^{1/3}\}$, also $\#\,A_n^{(1)} \le 2n^{1/3} + 1$.

Sei $A_n^{(2)} := \{\ell^2;\ \ell = \lfloor k^{1/2}n^{1/3}\rfloor$ oder $\ell = \lfloor k^{1/2}n^{1/3}\rfloor - 1,\ 4 \le k \le n^{1/3}\}$,

also $\#\,A_n^{(2)} \le 2\cdot(n^{1/3} - 3) = 2n^{1/3} - 6$.

Sei $A_n^{(0)} := A_n^{(1)} \cup A_n^{(2)}$. Dann ist $\#\,A_n^{(0)} < 4n^{1/3}$.

$A_n^{(0)}$ enthält alle $\square$e $\le 4n^{2/3}$.
Lagrange $\rightsquigarrow$ jede Zahl $m \le 4n^{2/3}$ ist Summe von vier Elementen von $A_n^{(0)}$. ✓

Fehlen noch folgende *m*: $4n^{2/3} < m \le n$?

- Sei $m \in \mathbb{N}$ mit $4n^{2/3} < m \le n,\ \underline{m \not\equiv 0\ (4)}$.

Beh. Es existiert ein $a_0 \in A_n^{(2)}$ mit $0 \le m - a_0^2 \le 4n^{2/3}$, und $m - a_0^2$ ist Summe 3er $\square$e (aus $A_n^{(1)}$).

$\ulcorner$ Sei $4 < k := \frac{m}{\lfloor n^{2/3} \rfloor} \le n^{1/3}$ und $a := \lfloor k^{1/2} n^{1/3} \rfloor$.

Dann ist $a^2 \in A_n^{(2)}$, $(a-1)^2 \in A_n^{(2)}$ und $a^2 \le kn^{2/3} \le m < (k+1)n^{2/3}$ sowie $a > k^{1/2}n^{1/3} - 1$.

Aus $(*)$ folgt: $m - a^2$ oder $m - (a-1)^2$ ist Summe 3er $\square$e. Wähle $a_0^2 \in \{(a-1)^2, a^2\} \subseteq A_n^{(2)}$, so daß $m - a_0^2$ Summe 3er $\square$e ist.
Da $4 < 3n^{1/6}$ für $n \ge 6$ folgt $0 \le m - a^2 \le m - a_0^2 \le m - (a-1)^2$

$$\begin{aligned} &< (k+1)\, n^{2/3} - (k^{1/2}n^{1/3} - 2)^2 < (k+1)\, n^{2/3} - kn^{2/3} + 4k^{1/2}n^{1/3} \\ &= n^{2/3} + 4k^{1/2}n^{1/3} \le n^{2/3} + 4n^{1/2} < 4n^{2/3}, \end{aligned}$$

also ist $m - a_0^2$ Summer 3er $\square$e aus $A_n^{(1)}$. $\lrcorner$

Also ist m Summe von 4 $\square$en aus $A_n^{(0)}$.

Fehlt noch, die m mit $4n^{2/3} < m \le n$ zu betrachten, die durch 4 teilbar sind! Und die genaue Definition von A_n! Diese ist wie folgt. (Rückführung auf $A_n^{(0)}$!)

- Sei nun $A_n := \{4^i a;\ 0 \le i \le \frac{\log n}{\log 4},\ a \in A_n^{(0)}\}$, d. h. $A_n^{(0)} \subseteq A_n$.
  Dann ist A_n Menge von $\square$en, und

$$\# A_n \le \Big(\frac{\log n}{\log 4} + 1\Big) \cdot \# A_n^{(0)} < \Big(\frac{2 \log n}{4}\Big) \cdot 4n^{1/3} = \Big(\frac{4}{\log 2}\Big) n^{1/3} \log n.$$

Sei $N \in [0, n]$.

Falls $N \not\equiv 0\ (4)$, ist N Summe von 4 $\square$en aus $A_n^{(0)} \subseteq A_n$, s. o.

Falls $N \equiv 0(4)$, ist $N = 4^i m$, mit $m \not\equiv 0(4)$, $0 \le i \le \frac{\log n}{\log 4}$.

Dann ist $m = a_1 + a_2 + a_3 + a_4$ mit Quadraten $a_1, \ldots, a_4 \in A_n^{(0)}$, s. o.,
also $N = 4^i m = 4^i a_1 + 4^i a_2 + 4^i a_3 + 4^i a_4$ eine Summe von 4 $\square$en aus a_n.

$\square$

Bemerkung. Es gibt eine Basis bezüglich 4 für n aus $\ll n^{1/4+\varepsilon}$ vielen $\square$en. Unbekannt ist, ob ε hier eliminiert werden kann. (Zöllner, 1985)

§ 3 Die Goldbachsche Vermutung und der Satz von Vinogradov

§ 3.1. Die Goldbachsche und Descartessche Vermutung

Aus dem Briefwechsel von 1742 zwischen Euler und Goldbach kann man folgende Fragen entnehmen:

(a) Ist jede gerade Zahl ≥ 4 Summe zweier Primzahlen? (*binäres Problem*)

(b) Ist jede ungerade Zahl ≥ 7 Summe dreier Primzahlen? (*ternäres Problem*)

1. Bem.: (a) $\Rightarrow$ (b), denn: $n \geq 7$ ungerade $\Rightarrow n-3 \geq 4$ gerade, $\overset{(a)}{\Rightarrow} n-3 = p_1+p_2 \Rightarrow n = 3+p_1+p_2$. D.h. (a) ist die stärkere, (b) die schwächere Vermutung. $\big[$(b) $\not\Rightarrow$ (a)$\big]$
Descartes hat schon früher (vor 1650) folgende Vermutung aufgestellt:

(c) Jede natürliche Zahl > 1 ist Summe von höchstens drei Primzahlen.

2. Bem.: Es gilt natürlich (a) $\Rightarrow$ (c), aber (b) $\overset{\not\Rightarrow}{\not\Leftarrow}$ (c), und auch **nicht** (c) $\Rightarrow$ (a), d. h. (a) und (c) sind **nicht** äquivalent. Vielmehr ist (c) äquivalent zu:

(d) Ist $n > 2$ gerade, so ist $n \in \mathcal{G}$ oder $n-2 \in \mathcal{G}$,
wobei $\mathcal{G} := \{g \in \mathbb{N}; \exists\, p_1, p_2 \text{ prim} : g = p_1+p_2\}$
die **Menge der Goldbachzahlen** sei.

⌜ (c) $\Rightarrow$ (d): $n > 2$ gerade $\overset{(c)}{\Rightarrow}$

$$\begin{cases} & n = p_1+p_2+p_3 \equiv 0(2),\ \text{d. h.} \quad p_1 = 2 \Rightarrow n-2 = p_2+p_3 \in \mathcal{G}\ \checkmark \\ \text{oder} & n = p_1+p_2 \Rightarrow n \in \mathcal{G}\ \checkmark \\ \text{oder} & n = p_1,\ \text{d. h.} \quad p_1 = 2 = n\ \lightning \end{cases}$$

(d) $\Rightarrow$ (c):

- Sei $n > 1$ ungerade, Œ $n > 5$. Dann ist $n-3 > 2$ gerade, also nach (d): $n-3 = p_1+p_2$ oder $n-3-2 = p_1+p_2$, d. h. $n = 3+p_1+p_2$ oder $n = 5+p_1+p_2$ ✓
- Sei $n > 1$ gerade, Œ $n > 2$. Nach (d) ist $n = p_1+p_2$ oder $n-2 = p_1+p_2 \Leftrightarrow n = 2+p_1+p_2$ ✓ ⌟

Bemerkung (3)**.** Descartes' Vermutung (c) bzw. (d) ist auch äquivalent zu folgender „Verschärfung":

(e) Jede natürliche Zahl > 1 ist Summe von höchstens drei Primzahlen, wobei der dritte Summand, falls existent, als 2, 3 oder 5 gewählt werden kann. (Einschränkung an einen Summanden sind daher von Interesse.)

⌜ Das sieht man im Beweis zu (d) $\Rightarrow$ (c). ⌟
Im Hinblick dazu: Die binäre Vermutung (a) ist äquivalent zu

(f) Jede natürliche Zahl > 5 ist Summe von drei Primzahlen, wobei der dritte Summand als 2 oder 3 gewählt werden kann.

⌜ (a) $\Rightarrow$ (f):

- $n > 4$ gerade $\overset{(a)}{\Rightarrow} 2 < n-2 = p_1 + p_2 \Rightarrow n = 2 + p_1 + p_2$ ✓
- $n > 5$ ungerade $\Rightarrow 2 < n-3$ gerade, also $\overset{(a)}{=} p_1 + p_2 \Rightarrow n = 3 + p_1 + p_2$ ✓

(f) $\Rightarrow$ (a): Sei $n > 2$ gerade $\overset{(f)}{\Rightarrow} n + 2 = p_1 + p_2 + p_3$, wobei aus Paritätsgründen und $(2 \mid p \Rightarrow p = 2)$ eine Primzahl $= 2$ sein muß. Also ist n Summe von 2 Primzahlen. ⌟

4. Bem.: Eine positive Antwort auf (a) ist sehr wahrscheinlich: Jedes n kann auf $n-1$ Arten als $m_1 + m_2$ geschrieben werden. Die Primzahlen treten mit einer relativen Häufigkeit $\approx (\log n)^{-1}$ auf (Primzahl–Satz), also hat ein gerades n vermutlich $\approx \frac{n}{(\log n)^2}$ viele Darstellungen als Summe zweier Primzahlen.
Obwohl sich dies numerisch gut bestätigen läßt, sind die Probleme (a)-(f) selbst sehr schwierig.

1937 löste Vinogradov das ternäre Problem (b) für alle hinreichend großen n. Seit 1997 weiß man, daß unter Annahme der verallgemeinerten Riemannschen Vermutung (GRH) das ternäre Problem (b) für **alle** $n \geq 7$ positiv zu beantworten ist. Das binäre Problem (a) $\Leftrightarrow$ (f) und das Descartessche Problem (c) $\Leftrightarrow$ (d) $\Leftrightarrow$ (e) sind bis heute offen. (Und (b), da auch die GRH offen...)
Allerdings sind bis heute außer (b) noch weitere „Approximationen“ an das binäre Problem bekannt, vor allem Verschärfungen des Vinogradovschen Satzes mit zusätzlichen Bedingungen an die Primzahlen, wie deren Vorgabe in Restklassen oder kurzen Intervallen, oder der Betrachtung der **Goldbach–Ausnahmen** $\mathcal{E}(x) := \{n \leq x;\ 2 \mid n \,\&\, n \notin \mathcal{G}\}$, für die $\#\,\mathcal{E}(x) \ll x^{\vartheta}$ mit einer positiven Konstanten $\vartheta < \frac{2}{3}$ gilt. [J. Pintz, '07]
Es gilt außerdem [J. Pintz '07]:
Bis auf $O(x^{3/5}(\log x)^{10})$ viele Ausnahmen lassen sich alle natürlichen Zahlen $\leq x$ schreiben als Summe von höchstens 3 Primzahlen, wobei die dritte (falls vorhanden) als 2,3 oder 5 gewählt werden kann. $\left[\text{Beachte } \frac{3}{5} < \frac{2}{3}\right]$

Die Goldbachsche und Descartessche Vermutung gelten also für „fast alle“ natürlichen Zahlen.

§ 3.2. Die Kreismethode von Hardy und Littlewood

Um 1920 entwickelten Hardy und Littlewood eine analytische Methode, die zur Lösung additiver Probleme herangezogen werden kann: die Kreismethode. Unter Annahme der GRH konnten sie das ternäre Goldbach-Problem (b) für alle hinreichend großen n lösen. Die Formulierung der Methode mit endlichen Exponentialsummen und deren genaue Analyse brachten Vinogradov dann 1937 zur Lösung des ternären Problems für $n \geq n_0$ ohne

Annahme einer unbewiesenen Vermutung. Wir werden die Methode und wie sie zum Beweis des Satzes von Vinogradov führt, hier ausführen.
Sei n groß und sei

$$r(n) := \sum_{\substack{p_1,p_2,p_3 \text{ prim} \\ p_1+p_2+p_3=n}} 1$$

die Anzahl Darstellungen, n als Summe dreier Primzahlen zu schreiben. Wie beim binären Problem (s. 4. Bem. in § 3.1.) läßt sich vermuten, daß

$$r(n) \approx \frac{n^2}{(\log n)^3}$$

gilt. Dies hat Vinogradov für alle $n \geq n_0$ beweisen können, genauer:

Satz 3.1. (Vinogradov) *Es gibt eine zahlentheoretische Funktion $\mathcal{S}(n)$ und positive Konstanten c_1, c_2 mit $c_1 < \mathcal{S}(n) < c_2$ für alle ungeraden n, so daß für alle $n \geq n_0$ gilt:*

$$r(n) = \mathcal{S}(n)\frac{n^2}{2(\log n)^3}\left(1 + \mathrm{O}\Big(\frac{\log\log n}{\log n}\Big)\right).$$

Die zahlentheoretische Funktion $\mathcal{S}(n)$ heißt **singuläre Reihe** für das ternäre Goldbach-Problem. Insbesondere folgt $r(n) > 0$ für alle hinreichend großen ungeraden n. Für gerade n ist jedoch $\mathcal{S}(n) = 0$, und somit ist mit Satz 3.1. $r(n) > 0$ nicht für gerade n zeigbar.

Die Grundidee zu einem Lösungsansatz mit der Kreismethode ist die folgende. Sei also $n \geq n_0$ hinreichend groß.

Definition: Für $\alpha \in \mathbb{R}$ sei

$$S(\alpha) = S(n,\alpha) := \sum_{p \leq n} \log p \; e(\alpha p),$$

und betrachte

$$R(n) := \sum_{p_1+p_2+p_3=n} \log p_1 \;\; \log p_2 \;\; \log p_3$$

als gewichtete Summe der Anzahl Darstellungen von n als Summe dreier Primzahlen.
Bem.: $e(\beta) := e^{2\pi i\beta}$ für $\beta \in \mathbb{R}$.

Die Gewichtung mit $\log p$ macht den Beweis technisch einfacher. Genau so gut kann man auch mit der von Mangoldt–Funktion Λ bewichten. Wir zeigen also erst eine asymptotische Formel für $R(n)$, aus der sich dann die für $r(n)$ später leicht herleiten läßt.

Die Exponentialsumme $S(\alpha)$ kann nun zur Berechnung von $R(n)$ dienen: Es gilt nämlich

$$R(n) = \sum_{p_1+p_2+p_3=n} \log p_1 \log p_2 \log p_3 \overset{!}{=} \int_0^1 S(\alpha)^3 \, e(-n\alpha)\, d\alpha,$$

denn die rechte Seite ist

$$= \sum_{p_1,p_2,p_3 \le n} \log p_1 \log p_2 \log p_3 \underbrace{\int_0^1 e(\alpha(p_1+p_2+p_3-n))d\alpha}_{\overset{\text{ONR}}{=} \begin{cases} 1, & p_1+p_2+p_3-n=0 \\ 0, & \text{sonst} \end{cases}} = R(n).$$

Die Idee der Kreismethode beruht nun auf der Beobachtung, daß der Wert des Integrals vor allem durch den Wert auf bestimmten Teilintervallen gegeben ist. Man nennt diese **maßgeblichen** Teilintervalle die „major arcs“ und die Restintervalle die „minor arcs“.

Beim ternären Goldbach-Problem wählt man die major arcs $\mathfrak{M} \subseteq [0,1]$ wie folgt.
Sei $B > 0$ und $Q := (\log n)^B$. Für $1 \le q \le Q$ und $0 \le a \le q$ mit $(a,q) = 1$ definiert man den major arc $\mathfrak{M}(a,q)$ als

$$\mathfrak{M}(a,q) := \left[\frac{a}{q} - \frac{Q}{n}, \frac{a}{q} + \frac{Q}{n}\right] \cap [0,1],$$

und die Vereinigung der major arcs als

$$\mathfrak{M} := \bigcup_{q=1}^{Q} \bigcup_{\substack{0 \le a \le q \\ (a,q)=1}} \mathfrak{M}(a,q) \subseteq [0,1].$$

1. Beh.: Die major arcs sind paarweise disjunkt für große n.

⌜ Ann. $\alpha \in \mathfrak{M}(a,q) \cap \mathfrak{M}(a',q')$ mit $\frac{a}{q} \neq \frac{a'}{q'}$. Dann ist $|aq' - a'q| \ge 1$ und

$$\frac{1}{Q^2} \le \frac{1}{qq'} \le \frac{|aq'-a'q|}{qq'} = \left|\frac{a}{q} - \frac{a'}{q'}\right| \le \left|\frac{a}{q} - \alpha\right| + \left|\alpha - \frac{a'}{q'}\right| \le 2\frac{Q}{n},$$

also $n \le 2Q^3 = 2(\log n)^{3B}$, was für alle hinreichend großen n nicht stimmt. $\rightsquigarrow$ ↯ ⌟

Die minor arcs definiert man also als $\mathfrak{m} := [0,1] \backslash \mathfrak{M}$. Somit spaltet man das $\int_0^1$ zur Berechnung von $R(n)$ auf in

$$R(n) = \int_{\mathfrak{M}} S(\alpha)^3 e(-n\alpha)\, d\alpha + \int_{\mathfrak{m}} S(\alpha)^3 e(-n\alpha)\, d\alpha.$$

Dieser Ansatz liefert dann eine asymptotische Formel: der Hauptterm ist in $\int_{\mathfrak{M}}$ enthalten, und $\int_{\mathfrak{m}}$ trägt nur zum Fehlerterm bei.
Wir beginnen im nächsten § 3.3 mit der Auswertung von $\int_{\mathfrak{M}}$.

§ 3.3. Auswertung der major arcs

Das nächste Lemma beschreibt das Verhalten der Exponentialsumme auf den major arcs.

Lemma 3.2. *Für $\alpha \in \mathfrak{M}$, $\alpha = \frac{a}{q} + \beta$, $q \le Q$, $(a,q) = 1$, $|\beta| \le \frac{Q}{n}$, gilt mit einem (universellen) $C > 0$:*

$$S(\alpha) = \frac{\mu(q)}{\varphi(q)} \sum_{m \le n} e(\beta m) + \mathrm{O}\big(n \exp(-C(\log n)^{1/10})\big).$$

Bemerkung. Die O–Konstante und C sind wegen der Verwendung des Satzes von Siegel–Walsfisz **nicht** numerisch angebbar.

Beweis. Zunächst ist für $\gamma \in \mathbb{R}$:

$$S(\gamma) = \sum_{\substack{r=1\\(r,q)=1}}^{q} \sum_{\substack{p \le n\\ p \equiv r(q)}} \log p \, e(\gamma p) + \mathrm{O}(\log q),$$

$$\text{da} \quad \sum_{\substack{r=1\\(r,q)>1}}^{q} \sum_{\substack{p \le n\\ p \equiv r(q)}} \log p = \sum_{\substack{p \le n\\ p \mid q}} \log p \ll \sum_{p \mid q} \log p \le \log q.$$

Also ist

$$\begin{aligned} S\Big(\frac{a}{q}\Big) &= \sum_{\substack{r=1\\(r,q)=1}}^{q} \sum_{\substack{p \le n\\ p \equiv r(q)}} \log p \, \overbrace{e\Big(\frac{ap}{q}\Big)}^{=e(\frac{ra}{q})} + \mathrm{O}(\log q) \\ &= \sum_{\substack{r=1\\(r,q)=1}}^{q} e\Big(\frac{ra}{q}\Big) \overbrace{\sum_{\substack{p \le n\\ p \equiv r(q)}} \log p}^{=\vartheta(n;q,r)} + \mathrm{O}(\log Q) \\ &= \sum_{\substack{r=1\\(r,q)=1}}^{q} e\Big(\frac{ra}{q}\Big) \vartheta(n;q,r) + \mathrm{O}(\log Q). \end{aligned}$$

Für $\vartheta(n;q,r)$ setzen wir nun die asymptotische Formel ein, die der **Satz von Siegel–Walfisz** liefert. Wir haben hier die Auswertung der Exponentialsumme auf das Problem der Primzahlverteilung in arithmetischen Progressionen aus der analytischen Zahlentheorie zurückgeführt. Mit $\vartheta(n;q,r) = \frac{n}{\varphi(q)} + \mathrm{O}\big(n \exp(-C_0(\log n)^{1/10})\big)$ erhalten wir also

$$S\Big(\frac{a}{q}\Big) = \sum_{\substack{r=1\\(r,q)=1}}^{q} e\Big(\frac{ra}{q}\Big) \cdot \Big(\frac{n}{\varphi(q)} + \mathrm{O}\big(n \exp(-C_0(\log n)^{1/10})\big)\Big) + \mathrm{O}(\log Q)$$

Die zahlentheoretische Funktion $c_q(a) := \sum\limits_{\substack{r=1\\(r,q)=1}}^{q} e\big(\frac{ra}{q}\big)$ heißt **Ramanujan–Summe**. Sie läßt sich hier berechnen durch

$$c_q(a) = \mu(q) \text{ für } (a,q) = 1.$$

⌜

$$c_q(a) = \sum_{\substack{r=1\\(r,q)=1}}^{q} e\Big(\frac{ra}{q}\Big) = \sum_{r=1}^{q} e\Big(\frac{ra}{q}\Big) \underbrace{\sum_{d|(r,q)} \mu(d)}_{=\begin{cases} 1, & (r,q)=1 \\ 0, & \text{sonst} \end{cases}} = \sum_{d|q} \mu(d) \sum_{\substack{r=1\\d|r}}^{q} e\Big(\frac{ra}{q}\Big)$$

$$= \sum_{d|q} \mu(d) \sum_{\ell=1}^{q/d} e\Big(\frac{\ell a}{q/d}\Big) = \sum_{d|q} \mu\Big(\frac{q}{d}\Big) \underbrace{\sum_{\ell=1}^{d} e\Big(\frac{\ell a}{d}\Big)}_{=\begin{cases} d, & \text{falls } d|a \\ 0, & \text{sonst} \end{cases}} = \sum_{\substack{d|q\\d|a}} \mu\Big(\frac{q}{d}\Big) d$$

$$= \sum_{\underbrace{d|(a,q)}_{\text{hier}=1}} \mu\Big(\frac{q}{d}\Big) d = \mu(q).$$

⌟

Somit ist

$$S\Big(\frac{a}{q}\Big) = \frac{\mu(q)}{\varphi(q)} \cdot n + \mathrm{O}\big(n \exp(-C_0(\log n)^{1/10})\big).$$

Um $S(\alpha)$ auszuwerten, wenden wir partielle Summation an und verwenden das Zwischenergebnis für $S\big(\frac{a}{q}\big)$:

Sei $\lambda(m) := \begin{cases} \log p, & \text{falls} \quad m = p \text{ prim}, \\ 0, & \text{sonst} \end{cases}$.

Damit ist

$$S(\alpha) - \frac{\mu(q)}{\varphi(q)} \sum_{m\le n} e(\beta m) = \sum_{m\le n} \lambda(m) \underbrace{e(\alpha m)}_{=e(\frac{ma}{q})e(m\beta)} - \frac{\mu(q)}{\varphi(q)} \sum_{m\le n} e(\beta m)$$

$$= \sum_{m\le n} \underbrace{\Big(\lambda(m) e\Big(\frac{ma}{q}\Big) - \frac{\mu(q)}{\varphi(q)}\Big)}_{=:\, a(m) \text{ für partielle} \sum} e(\beta m).$$

Nun ist für $x \ge 1$:

$$\sum_{m\le x} a(m) = \sum_{m\le x} \lambda(m) e\Big(\frac{ma}{q}\Big) - \frac{\mu(q)}{\varphi(q)} \cdot x + \overbrace{\mathrm{O}\Big(\frac{1}{\varphi(q)}\Big)}^{\text{von } \lfloor x\rfloor = x + \mathrm{O}(1)}$$

$$= S\Big(\frac{a}{q}, x\Big) - \frac{\mu(q)}{\varphi(q)} \cdot x + \mathrm{O}(1) = \mathrm{O}\big(x \exp(-C_0(\log x)^{1/10})\big),$$

also ist (partielle Summation):

$$S(\alpha) - \frac{\mu(q)}{\varphi(q)} \sum_{m \le n} e(\beta m) = e(\beta n) \sum_{m \le n} a(m) - \underbrace{2\pi i \beta \int_1^n e(\beta x) \sum_{m \le x} a(m) dx}_{\ll \underbrace{|\beta| n}_{\le Q = (\log n)^B} \max_{x \le n} \{ \big| \sum_{m \le x} a(m) \big| \}}$$

$$\ll n \exp\big(- C(\log n)^{1/10}\big),$$

mit einer Konstante $C > 0$, die von B und C_0 abhängt. □

Nun sind wir soweit, daß wir das Integral über $\mathfrak{M}$ auswerten können:

Satz 3.3. *Für beliebige $A > 0$ ist für eine Konstante $B = B(A) > 0$ und $Q := (\log n)^B$:*

$$\int_{\mathfrak{M}} S^3(\alpha) e(-n\alpha) d\alpha = \mathcal{S}(n) \frac{n^2}{2} + \mathrm{O}\Big(\frac{n^2}{(\log n)^A}\Big),$$

wobei die O*–Konstante nur von A abhängt. Dabei ist*

$$\mathcal{S}(n) := \sum_{q=1}^{\infty} \frac{\mu(q) c_q(-n)}{\varphi(q)^3} \quad \textit{die } \textbf{singuläre Reihe}$$

des ternären Goldbachproblems.

Beweis. Sei $\alpha \in \mathfrak{M}(a,q)$, $\beta := \alpha - \frac{a}{q}$. Aus der Formel für $S(\alpha)$ folgt

$$S(\alpha)^3 = \frac{\mu(q)}{\varphi(q)^3} \Big(\sum_{m \le n} e(\beta m) \Big)^3 + \mathrm{O}\big(n^3 \exp(-C(\log n)^{1/10})\big),$$

da ja $\sum_{m \le n} e(\beta m) \ll n$ ist. (Und $\mu^3 = \mu$.)
Also ist

$$\int_{\mathfrak{M}} S(\alpha)^3 e(-n\alpha) d\alpha = \sum_{q \le Q} \sum_{\substack{0 \le a \le q \\ (a,q)=1}} \underbrace{\int_{\mathfrak{M}(a,q)}}_{(\text{IVlänge } \frac{2Q}{n})} \frac{\mu(q)}{\varphi(q)^3} \Big(\sum_{n \le n} e\Big(\Big(\alpha - \frac{a}{q} \Big) m \Big) \Big)^3 e(-n\alpha) d\alpha$$

$$+ \mathrm{O}\Big(\frac{Q^3}{n} \cdot n^3 \exp\big(- C(\log n)^{1/10} \big) \Big)$$

$$= \sum_{q\le Q} \frac{\mu(q)}{\varphi(q)^3} \sum_{\substack{0\le a\le q\\(a,q)=1}} e\Big(-n\frac{a}{q}\Big) \int\limits_{\frac{a}{q}-\frac{Q}{n}}^{\frac{a}{q}+\frac{Q}{n}} \Big(\sum_{m\le n} e\Big(\underbrace{\Big(\alpha-\frac{a}{q}\Big)}_{\beta} m\Big)\Big)^3 e\Big(-n\underbrace{\Big(\alpha-\frac{a}{q}\Big)}_{\beta}\Big) d\alpha + \mathrm{O}\Big(\frac{n^2}{(\log n)^A}\Big)$$

$$= \sum_{q\le Q} \frac{\mu(q)}{\varphi(q)^3}\, c_q(-n) \cdot \int\limits_{-Q/n}^{Q/n} \Big(\sum_{m\le n} e\big(\beta m\big)\Big)^3 e(-n\beta)\, d\beta + \mathrm{O}\Big(\frac{n^2}{(\log n)^A}\Big)$$

$$= \mathcal{S}(n,Q) \cdot \int\limits_{-Q/n}^{Q/n} \Big(\sum_{m\le n} e\big(\beta m\big)\Big)^3 e(-n\beta)\, d\beta + \mathrm{O}\Big(\frac{n^2}{(\log n)^A}\Big),$$

wobei wir $\mathcal{S}(n,Q) := \sum_{q\le Q} \frac{\mu(q)}{\varphi(q)^3} c_q(-n)$ gesetzt haben.

Das verbleibende Integral splitten wir auf in $\int\limits_{-1/2}^{1/2} - \int\limits_{Q/n}^{1/2} - \int\limits_{-1/2}^{-Q/n}$. Da

$$\sum_{m\le n} e(\beta m) \ll \frac{1}{|\beta|} \text{ für } |\beta| \le \frac{1}{2} \text{ gilt (s. § 1.3)},$$

ist das 2. Integral

$$= \int\limits_{Q/n}^{1/2} \Big(\sum_{m\le n} e(\beta m)\Big)^3 e(-n\beta)\, d\beta \ll \int\limits_{Q/n}^{1/2} \frac{1}{\beta^3}\, d\beta < \frac{n^2}{Q^2}$$

und das 3. Integral ebenso $\ll \dfrac{n^2}{Q^2}$.

Weiter ist

$$\int\limits_{-1/2}^{1/2} \Big(\sum_{m\le n} e(\beta m)\Big) e(-n\beta)\, d\beta = \sum_{m_1\le n} \sum_{m_2\le n} \sum_{m_3\le n} \underbrace{\int\limits_{-1/2}^{1/2} e((m_1+m_2+m_3-n)\beta) d\beta}_{\underset{\text{ONR}}{=} \begin{cases} 1, & m_3 = n-m_1-m_2 \\ 0, & \text{sonst.} \end{cases}}$$

$$= \sum_{m_1\le n} \sum_{\substack{m_2\le n\\ n-m_1>m_2}} 1 = \sum_{m_1\le n-2} (n-m_1-1)$$

$$= \sum_{k=1}^{n-2} k = \frac{1}{2}(n-2)(n-1) = \binom{n-1}{2} = \frac{n^2}{2} + \mathrm{O}(n),$$

also $\int\limits_{-Q/n}^{Q/n} \cdots = \frac{n^2}{2} + \mathrm{O}\Big(\frac{n^2}{Q^2}\Big)$. Es folgt

$$\begin{aligned}\int\limits_{\mathfrak{M}} S(\alpha)^3 e(-n\alpha)d\alpha &= \mathcal{S}(n,Q)\cdot\frac{n^2}{2} + \mathrm{O}\Big(\frac{n^2}{Q^2}\Big) + \mathrm{O}\Big(\frac{n^2}{(\log n)^A}\Big)\\ &= \mathcal{S}(n,Q)\cdot\frac{n^2}{2} + \mathrm{O}\Big(\frac{n^2}{(\log n)^A}\Big) \text{ für } B = B(A) > 0.\end{aligned}$$

Die im Hauptterm vorkommenden endlichen Summen sind die Partialsummen der **singulären Reihe**

$$\mathcal{S}(n) = \sum_{q=1}^{\infty} \frac{\mu(q)c_q(-n)}{\varphi(q)^3} = \lim_{Q\to\infty} \mathcal{S}(n,Q),$$

die wegen

$$\sum_{q\le Q} \frac{\mu(q)\overbrace{c_q(-n)}^{\ll\varphi(q)}}{\varphi(q)^3} \ll \sum_{q\le Q} \frac{1}{\varphi(q)^2}$$

absolut konvergiert, auch gleichmäßig in n.

Denn da $\varphi(q) > q^{1-\varepsilon/2}$ für $\varepsilon > 0$ und alle hinreichend großen q (vgl. (Ü)), etwa $\varepsilon := \frac{1}{2}$, folgt

$$\mathcal{S}(n) - \mathcal{S}(n,Q) \ll \sum_{q>Q} \frac{1}{\varphi(q)^2} \ll \sum_{q>Q} \frac{1}{q^{2-\varepsilon}} \ll \frac{1}{Q^{1-\varepsilon}}.$$

Mit $Q = (\log n)^B$ und $B(A)$ geeignet erhalten wir

$$\int\limits_{\mathfrak{M}} S(\alpha)^3 e(-n\alpha)d\alpha = \mathcal{S}(n)\frac{n^2}{2} + \mathrm{O}\Big(\frac{n^2}{(\log n)^A}\Big),$$

die Behauptung. □

Die singuläre Reihe $\mathcal{S}(n)$ wollen wir noch genauer daraufhin untersuchen, ob sie $= 0$ sein könnte. Dann wäre der Hauptterm ja wertlos im Vergleich zum angegebenen Fehlerterm. Dafür entwickeln wir eine andere Formel für $\mathcal{S}(n)$:

Satz 3.4. *Es gilt*

$$\mathcal{S}(n) = \prod_{p\nmid n}\Big(1 + \frac{1}{(p-1)^3}\Big)\cdot\prod_{p|n}\Big(1 - \frac{1}{(p-1)^2}\Big).$$

Insbesondere ist also $\mathcal{S}(n) = 0$ für gerade n, und es gibt Konstanten $c_1, c_2 > 0$, so daß $c_1 < \mathcal{S}(n) < c_2$ für alle ungeraden n.

Man nennt diese Produktdarstellung das **Euler-Produkt** für $\mathcal{S}(n)$, in Anlehnung an die Euler-Produkt-Entwicklung von $\displaystyle\sum_{n,p|n\Rightarrow p\le N} \frac{1}{n} = \prod_{p\le N}\Big(1-\frac{1}{p}\Big)^{-1}$. **Genauer:** Ist f eine multiplikative zahlentheoretische Funktion und $\sum\limits_{n=1}^{\infty} f(n)$ absolut konvergent, dann ist

$$\sum_{n=1}^{\infty} f(n) = \prod_{p}\Big(\sum_{k=0}^{\infty} f(p^k)\Big).$$

Ist f sogar vollständig multiplikativ, so ist

$$\sum_{n=1}^{\infty} f(n) = \prod_{p}\big(1-f(p)\big)^{-1}. \quad \textbf{(Euler-Produkt-Satz)}$$

Beweis. (von Satz 3.4) Die zahlentheoretische Funktion $\frac{\mu(q)c_q(-n)}{\varphi(q)^3}$ ist multiplikativ in q, da $c_q(-n)$ multiplikativ in q ist [vgl. (Ü)]. Weiter ist

$$c_p(-n) = \sum_{1\le a<p} e\Big(\frac{-an}{p}\Big) = \begin{cases} p-1, & p \mid n, \\ -1, & \text{sonst.} \end{cases}$$

Der Euler-Produkt-Satz liefert also

$$\mathcal{S}(n) = \prod_{p}\Big(1+\sum_{k=1}^{\infty}\underbrace{\frac{\mu(p^k)c_{p^k}(-n)}{\varphi(p^k)^3}}_{=0 \text{ für } k\ge 2}\Big) = \prod_{p}\Big(1-\frac{c_p(-n)}{\varphi(p)^3}\Big)$$

$$= \prod_{p\nmid n}\Big(1+\frac{1}{(p-1)^3}\Big)\prod_{p\mid n}\Big(1-\frac{1}{(p-1)^2}\Big). \quad [\text{Konvergiert für } 2\nmid n]$$

□

Damit ist die Behandlung der major arcs abgeschlossen. Beachtlich ist, daß diese den Hauptterm der asymptotischen Formel liefern, denn deren Maß ist nur

$$2\sum_{q\le Q}\sum_{\substack{0\le a\le q\\(a,q)=1}}\frac{Q}{n} \ll \frac{Q^3}{n} = \frac{(\log n)^{3B}}{n} \overset{n\to\infty}{\longrightarrow} \mathrm{O}.$$

Daß die großen minor arcs nur noch zum Fehlerterm beitragen und deren Beitrag klein bleibt, ist das schwierigere Problem und wird in den nächsten § 3.4. und § 3.5. behandelt.

§ 3.4. Auswertung der minor arcs

Das Verhalten der Exponentialsumme $S(\alpha)$ auf $\mathfrak{m}$ beschreibt der folgende Satz von Vinogradov, den wir mit Vaughans Identiät beweisen werden. Diese wurde später, nach Vinogradov, von Vaughan entwickelt und vereinfacht die Abschätzungen von Vinogradov wesentlich.

Satz 3.5. (Vinogradov, Vaughan) *Gilt* $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}$, *wo* $1 \leq q \leq n,\ (a,q) = 1$, *so ist*

$$S(\alpha) \ll \left(\frac{n}{q^{1/2}} + n^{4/5} + n^{1/2}q^{1/2}\right)(\log n)^4.$$

Bemerkung. Für $\alpha \in \mathfrak{m}$ liefert dieser Satz eine nichttriviale obere Abschätzung für $S(\alpha)$. Um das einzusehen, brauchen wir zunächst den (auch sonst für die Zahlentheorie wichtigen)

Satz 3.6. (Approximationssatz von Dirichlet) *Zu jedem* $\alpha \in \mathbb{R}$ *und* $X \in \mathbb{R}_{>1}$ *existiert* $q \in \mathbb{N},\ a \in \mathbb{Z},\ 1 \leq q \leq X$, $(a,q) = 1$, *so daß* $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{qX}$ *gilt.*

Beweis. Zu lösen ist $\left|\alpha q - a\right| \leq \frac{1}{X}$.
Man zerlege das Intervall $[0,1]$ in $[X]+1$ viele disjunkte Teilintervalle der Länge $\big([X]+1\big)^{-1}$ und betrachte die $\{\alpha q\} = \alpha q - [\alpha q]$ mit $q \leq X$ darin.

1. Fall (Randfall) Es existiert q mit A) $\{\alpha q\} \in [\,0, ([X]+1)^{-1}\big[$ oder B) $\in \big[[X]/([X]+1), 1\big]$
$\rightsquigarrow$ dieses q tut es mit A) $a := [\alpha q]$, da $0 \leq \{\alpha q\} = \alpha q - a < \frac{1}{[X]+1} \leq \frac{1}{X}$
bzw. mit B) $a := [\alpha q] + 1$, da $\frac{[X]}{[X]+1} \leq \{\alpha q\} = \alpha q - a + 1 < 1$.

2. Fall Existiert kein solches q, so liegen die $\{\alpha q\}$ für $q = 1, \ldots, [X]$ in einem der $[X] - 1$ vielen Intervalle $\big[\frac{i}{[X]+1}, \frac{i+1}{[X]+1}\big[$ für $i = 1, \ldots, [X]-1$. Nach dem Dirichletschen Schubfachprinzip gibt es also ein Intervall, in dem zwei der $\{\alpha q\}$ liegen, d. h. es existiert $i \in \{1, \ldots, [X]-1\}$, und $q_1, q_2 \in \big\{1, \ldots [X]\big\}$ mit $1 \leq q_1 < q_2 \leq [X]$: $\{\alpha q_1\}, \{\alpha q_2\} \in \big[\frac{i}{[X]+1}, \frac{i+1}{[X]+1}\big[$. Sei $q := q_2 - q_1,\ a := [\alpha q_2] - [\alpha q_1]$, dann ist

$$|\alpha q - a| = |\alpha q_2 - [\alpha q_2] - (\alpha q_1 - [\alpha q_1])| = |\{\alpha q_2\} - \{\alpha q_1\}| < \frac{1}{[X]+1} \leq \frac{1}{X}.$$

Ist der so erhaltene Bruch $\frac{a}{q}$ noch ungekürzt, so kürze man ihn zu $\frac{a'}{q'}$ mit $(a',q') = 1$ und erhält so

$$\left|\alpha - \frac{a'}{q'}\right| \leq \frac{1}{qX} \leq \frac{1}{q'X}.$$

□

Für ein $\alpha \in \mathfrak{m}$ garantiert Satz 3.6. die Existenz eines Bruches $\frac{a}{q}, (a,q) = 1$, mit $q \leq \frac{n}{Q}$ und $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{qn/Q} = \frac{Q}{qn}$ also $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}$. Da $\alpha \in \mathfrak{m}$, gilt für dieses q dann $q > Q = (\log n)^B$, denn sonst wäre ja $\alpha \in \mathfrak{M}(a,q) \subseteq \mathfrak{M}$ ↯.

Nach dem Approximationssatz von Dirichlet können wir auch die Punkte α der minor arcs mit Brüchen annähern, deren Nenner haben dann aber eine gewisse Mindestgröße Q, da sie ja nicht auf den major arcs liegen, die durch Brüche mit kleinen Nenner approximiert werden können.
Da q also in dem Bereich $\in \left[Q, \frac{n}{Q}\right]$ liegt, wird die Abschätzung in Satz 3.5. dann offenbar eine nichttriviale obere Schranke für $S(\alpha)$ auf $\mathfrak{m}$ liefern. [Trivial wäre die obere Schranke $S(\alpha) \ll n$.]

Wir entwickeln nun das zentrale Hilfsmittel zum Beweis von 3.5., die Vaughansche Identität:

Satz 3.7. (Vaughans Identität) *Für eine zahlentheoretische Funktion f und $U \in \mathbb{R}$ ist*

$$\sum_{m\le n} \Lambda(m) f(m) = S_1 + S_2 + S_3 + S_4$$

mit

$$S_i = \sum_{m\le n} a_i(m) f(m) \text{ für } i = 1, \dots, 4, \text{ wobei}$$

$$a_1(m) := \left\{ \begin{array}{ll} \Lambda(m), & m \le U \\ 0, & m > U \end{array} \right\}, \quad a_2(m) := -\sum_{\substack{\ell j \mid m \\ \ell, j \le U}} \Lambda(\ell)\mu(j),$$

$$a_3(m) := \sum_{\substack{k\ell = m \\ \ell \le U}} \mu(\ell) \log k, \quad a_4(m) := -\sum_{\substack{jk = m \\ j > U, k > 1}} \Lambda(j) \cdot \sum_{\substack{d \mid k \\ d \le U}} \mu(d).$$

Beweis. Natürlich ginge der Beweis auch völlig elementar; wir zeigen hier aber einen analytischen Beweis, der einfacher und wesentlich eleganter ist:
Sei für $\operatorname{Re} s > 1$: $F(s) := \sum\limits_{m\le U} \frac{\Lambda(m)}{n^s}$, $G(s) := \sum\limits_{m\le U} \frac{\mu(m)}{m^s}$. Dies sind alles Beispiele für Partialsummen von Dirichletreihen; die Untersuchung analytischer Eigenschaften von Dirichletreihen sind ja zentrales Thema der analytischen Zahlentheorie. So hat man etwa für $\operatorname{Re} s > 1$ die Dirichletreihen

$$\zeta(s) = \sum_{m\ge 1} \frac{1}{m^s}, \ \zeta'(s) = \sum_{m\ge 1} \frac{-\log m}{m^s}, \ -\frac{\zeta'}{\zeta}(s) = \sum_{n\ge 1} \frac{\Lambda(m)}{m^s} \ (\text{da } \Lambda * \underline{1} = \log).$$

Denn multipliziert man zwei Dirichletreihen miteinander, so werden ihre Koeffizienten zahlentheoretisch gefaltet. Mit der Identität

$$-\frac{\zeta'}{\zeta}(s) = F(s) - \zeta(s)F(s)G(s) - \zeta'(s)G(s) + \Big(-\frac{\zeta'}{\zeta}(s) - F(s)\Big)\big(1 - \zeta(s)G(s)\big)$$

von Dirichletreihen folgern wir aus dem Identitätssatz (der ähnlich wie für Potenzreihen auch für Dirichletreihen gilt), daß deren Koeffizienten links und rechts gleich sind, also ist

$$\Lambda(m) = a_1(m) + a_2(m) + a_3(m) + a_4(m) \quad \text{(auch oft „Vaughansche Identität“ genannt)}$$

mit den angegebenen zahlentheoretischen Funktionen $a_i(m)$ als Faltung der entsprechenden Koeffizienten der Dirichletreihen der Identität, die als Faktoren auftauchen. Multiplikation mit $f(m)$ und $\sum\limits_{m\le n}$ über die Identität für $\Lambda(m)$ liefert die Behauptung. □

Damit können wir Abschätzungen von Summen der Form $\sum\limits_{m\le n} f(m)\Lambda(m)$ vornehmen (anwenden werden wir dies auf die Exponentialsumme $\tilde{S}(\alpha) := \sum_{m\le n}\Lambda(m)e(\alpha m)$, die sehr nahe an $S(\alpha)$ ist):

Satz 3.8. *Sei $1 \le U \le n^{1/2}$. Dann gilt für jede zahlentheoretische Funktion f die Abschätzung*

$$\sum_{U<m\le n} f(m)\Lambda(m) \ll (\log n)T_1' + T_2'$$

mit

$$T_1' := \sum_{\ell\le U^2}\max_w\Big|\sum_{w<k\le\frac{n}{\ell}} f(k\ell)\Big|,$$
$$T_2' := \Big|\sum_{U<m<\frac{n}{U}}\ \sum_{U<k\le\frac{n}{m}} \Lambda(m)b(k)f(mk)\Big|,$$

Wobei $b(k)$ eine zahlentheoretische Funktion ist mit $\big|b(k)\big| \le d(k)\,(\forall k)$, die nur von U abhängt.

Beweis. Die linke Seite ist $= S_2+S_3+S_4$ in Vaughans Identität. Wir schätzen die Summen S_3, S_4, S_2 nach oben ab:

(S_3:) Mit $\log k = \int\limits_1^k \frac{dy}{y}$ haben wir

$$S_3 = \int\limits_{m\le n}\ \sum_{\substack{k\ell=m\\ \ell\le U}}\mu(\ell)\Big(\int\limits_1^k\frac{dy}{y}\Big)f(k\ell) = \sum_{\ell\le U}\mu(\ell)\sum_{k\le\frac{n}{\ell}} f(k\ell)\ \underbrace{\int\limits_1^k\frac{dy}{y}}_{=\sum_{j\le k-1}\int_j^{j+1}\frac{dy}{y}}$$

$$= \sum_{\ell\le U}\mu(\ell)\sum_{j\le\frac{n}{\ell}-1}\int\limits_j^{j+1}\ \underbrace{\sum_{j<k\le\frac{n}{\ell}}}_{\rightsquigarrow\ y<k} f(k\ell)\cdot\frac{dy}{y}$$

$$= \underbrace{\sum_{j\le n-1}\int\limits_j^{j+1}}_{\rightsquigarrow\int_1^n}\ \underbrace{\sum_{\substack{\ell\le U\\ \ell\le\frac{n}{j+1}}}}_{\rightsquigarrow\sum_{\ell\le\min\{U,\frac{n}{j+1}\}}}\ \mu(\ell)\sum_{y<k\le\frac{n}{\ell}} f(k\ell)\frac{dy}{y}$$

$$\ll (\log n) \sum_{\ell \le U} \max_w \Big| \sum_{w < k \le \frac{n}{\ell}} f(k\ell) \Big| \ll T_1'(\log n).$$

(S_2:) Diese Summe läßt sich wie S_3 abschätzen: Wir haben

$$S_2 = \sum_{m \le n} \Big(- \sum_{\substack{k\ell j = m \\ \ell, j \le U}} \Lambda(\ell)\mu(j) f(k \underbrace{\ell j}_{=:t}) \Big) = - \sum_{t \le U^2} \Big(\overbrace{\sum_{\substack{\ell j = t \\ \ell, j \le U}} \Lambda(\ell)\mu(j)}^{\alpha(t):=} \Big) \sum_{k \le \frac{n}{t}} f(kt).$$

Dies ist auch $\ll (\log n) T_1'$, da

$$\big|\alpha(t)\big| \le \sum_{\ell \mid t} \Lambda(\ell) = \log t \le \log n \text{ ist mit } U^2 \le n.$$

(S_4:) Wegen $\sum_{\substack{d \mid k \\ d \le U}} \mu(d) = 0$ für $1 < k \le U \quad [\mu * \underline{1} = \varepsilon]$ folgt

$$S_4 = - \sum_{U < j \le \frac{n}{U}} \sum_{U < k \le \frac{n}{j}} \Lambda(j) \underbrace{\Big(\sum_{\substack{d \mid k \\ d \le U}} \mu(d) \Big)}_{=:\, b(k) \text{ für } k > U} f(jk),$$

also $S_4 \ll T_2'$ mit $\big|b(k)\big| \ll d(k)$. □

Wir können damit nun den Satz 3.5 von Vinogradov/Vaughan beweisen:

Beweis. (von 3.5.) Sei $\alpha \in \mathbb{R}$ und dazu $(a,q) = 1,\ 1 \le q \le n$ mit $\big|\alpha - \frac{a}{q}\big| \le \frac{1}{q^2}$.
Dann wenden wir 3.8. an auf $f(k) = e(\alpha k)$: Es folgt für $1 \le U \le n^{1/2}$:

$$\tilde{S}(\alpha) := \sum_{m \le n} \Lambda(m) e(\alpha m) \ll U + (\log n) T_1 + T_2,$$

wo

$$T_1 = \sum_{\ell \le U^2} \max_w \Big| \sum_{w \le k \le \frac{n}{\ell}} e(\alpha k \ell) \Big| \ll \sum_{\ell \le U^2} \min \Big(\frac{n}{\ell}, \|\alpha\|^{-1} \Big)$$

(Abschnitt einer geometrischen Summe, vgl. §1.3) und

$$T_2 = \Big| \sum_{U < j \le \frac{n}{U}} \sum_{U < k \le \frac{n}{j}} \Lambda(j) b(k) e(\alpha j k) \Big| \text{ ist.}$$

Auch T_2 wollen wir so abschätzen wie T_1, nämlich mit einer geometrischen Summe. Dazu vertauschen wir $\sum_j$ mit $\sum_k$ und zerlegen die äußere $\sum_k$ in Abschnitte $K < k \le 2K$ für

$K = 2^v \cdot U$ mit $K \le \frac{n}{U}$, d. h. $v = 1, \dots, \lfloor \frac{\log(\frac{n}{U^2})}{\log 2} \rfloor$.
Da $v \ll \log n$ folgt

$$T_2 \ll (\log n) \max_{U \le K \le \frac{n}{U}} T(K)$$

mit $T(K) = \Big| \sum_{K<k\le 2K} b(k) \cdot \sum_{U<j\le \frac{n}{k}} \Lambda(j) e(\alpha j\, k) \Big|$.
Wir wenden darauf die Cauchy-Schwarzsche Ungleichung an und erhalten somit

$$T(K)^2 \le \underbrace{\Big(\sum_{k\le 2K} \big|b(k)\big|^2 \Big)}_{\le \sum_{k\le 2K} d(k)^2 \ll K(\log K)^3 \quad (\ddot{\text{U}})} \cdot \sum_{K<k\le 2K} \Big| \sum_{U<j\le \frac{n}{k}} \Lambda(j) e(\alpha j k) \Big|^2$$

$$\ll K(\log K)^3 \sum_{K<k\le 2K} \sum_{U<j_1,j_2\le \frac{n}{k}} \Lambda(j_1)\Lambda(j_2) e\big(\alpha k(j_1 - j_2)\big).$$

Hier separieren wir die Terme mit $j_2 = j_1$, deren Beitrag $\ll K(\log K)^3 \cdot K \cdot \frac{n}{K} \cdot (\log n)^2 \ll Kn(\log n)^5$ bringt, von denen mit $j_2 \ne j_1$, es folgt:

$$T(K)^2 \ll Kn(\log n)^5 + K(\log n)^5 \cdot \sum_{U<j_2<j_1\le \frac{n}{K}} \min\big(K, \|\alpha(j_1 - j_2)\|^{-1}\big),$$

da die $\sum_k e\big(\alpha k(j_1 - j_2)\big)$ wiederum eine geometrische Summe war.
Setzen wir $\ell := j_1 - j_2$, so ist $1 \le \ell \le \frac{n}{K}$, und zu einem ℓ gibt es $\le \frac{n}{K}$ viele Paare (m_1, m_2) mit $\ell = m_2 - m_1$, also folgt

$$T(K)^2 \ll Kn(\log n)^5 + n(\log n)^5 \sum_{\ell\le \frac{n}{K}} \min\Big(\frac{n}{\ell}, \|\alpha\ell\|^{-1}\Big).$$

Die verbleibenden Summen können wir nun mit folgendem Lemma behandeln. □

Lemma 3.9. *Sei* $\big|\alpha - \frac{a}{q}\big| \le \frac{1}{q^2}, (a,q) = 1,\ q, L \ge 1,\ n > 1$. *Dann:*

$$\sum_{\ell\le L} \min\Big(\frac{n}{\ell}, \|\alpha\ell\|^{-1}\Big) \ll \Big(\frac{n}{q} + L + q\Big) \log(2Lq).$$

Damit ist dann

$$T(K) \ll (Kn)^{1/2} (\log n)^{5/2} + \Big(\frac{n}{q^{1/2}} + \frac{n}{K^{1/2}} + (nq)^{1/2}\Big)(\log n)^3 \text{ für } q \le n,$$

$$\text{also} \qquad T_2 \ll (\log n)^4 \cdot \Big(\frac{n}{q^{1/2}} + \frac{n}{U^{1/2}} + (nq)^{1/2}\Big)$$

$$\text{und} \qquad T_1 \ll (\log n)\cdot\Big(\frac{n}{q^{1/2}} + U^2 + (nq)^{1/2}\Big).$$

Setzt man nun $U := n^{2/5}$, so ist $\frac{n}{U^{1/2}} = U^2 = n^{4/5}$, und wir haben

$$\tilde{S}(\alpha) \ll U + (\log n)\,T_1 + T_2 \ll (\log n)^4\cdot\Big(\frac{n}{q^{1/2}} + n^{4/5} + (nq)^{1/2}\Big).$$

Wegen

$$\tilde{S}(\alpha) - S(\alpha) = \sum_{\substack{p^k\le n\\ k\ge 2}} \log p\; e(\alpha p) \ll \sum_{p\le n^{1/2}}\ \sum_{k\le \frac{\log n}{\log p}} \log p \ll \sum_{p\le n^{1/2}} \log n \ll n^{1/2}\log n$$

folgt diese Abschätzung dann auch für $S(\alpha)$. $\square$ Beweisende von Lemma 3.5.

Bleibt noch, den Beweis des Lemmas 3.9. zu bringen:

Beweis. (von 3.9.) Sei $\beta := \alpha - \frac{a}{q}$, also $|\beta| \le \frac{1}{q^2},\ \alpha = \frac{a}{q} + \beta$.
Schreibe $\ell = hq + r$ mit $1 \le r \le q$ (Div. mit Rest), dann ist die linke Seite

$$= \sum_{\ell\le L} \min\Big(\frac{n}{\ell}, \|\alpha\ell\|^{-1}\Big) \le \sum_{0\le h<\frac{L}{q}}\ \sum_{1\le r\le q} \min\Big(\frac{n}{hq+r}, \Big\|\frac{ra}{q} + hq\beta + r\beta\Big\|^{-1}\Big)$$

1. Fall $r \le \frac{q}{2}$ (also $|r\beta| \le \frac{1}{2q}$) und $h = 0$.

Der Beitrag dieser Summanden ist

$$\ll \sum_{r\le q/2} \Big(\underbrace{\Big\|\frac{ra}{q}\Big\|}_{=:s(r)/q} - \frac{1}{2q}\Big)^{-1} = \sum_{r\le q/2}\Big(\frac{s(r)}{q} - \frac{1}{2q}\Big)^{-1}$$

wobei $s(r) \le q/2$ ist, sowie $s(r) \ge 1$ da $s(r) = 0 \Leftrightarrow q \mid r$ im $\lightning$ zum 1. Fall.
Da nun

$$\Big\{\frac{s(r)}{q};\ r \le \frac{q}{2}\Big\} = \Big\{\frac{s}{q};\ s \le \frac{q}{2}\Big\} \qquad (*)$$

gilt, folgt für den Beitrag der Summanden im 1. Fall

$$\ll \sum_{1\le s\le q/2}\Big(\frac{s}{q} - \frac{1}{2q}\Big)^{-1} = 2q\sum_{1\le s\le q/2}\frac{1}{2s-1} \le 2q\sum_{s\le q/2}\frac{1}{s} \ll q\log q,$$

dieser ist also klein genug.

$\ulcorner$ Begründung zur Gleichung (*):

$\subseteq$ ist klar, und die Anzahl der Elemente links und rechts ist gleich, nämlich $= \lfloor q/2\rfloor$, da gilt:

$$s(r_1) = s(r_2) \Leftrightarrow \|\frac{ar_1}{q}\| = \|\frac{ar_2}{q}\| \Leftrightarrow ar_1 \equiv \pm ar_2(q)$$
$$\Leftrightarrow r_1 \equiv \pm r_2(q) \text{ da } (a,q) = 1 \Leftrightarrow r_1 = r_2 \text{ da } 1 \le r_1, r_2 \le q/2. \qquad \lrcorner$$

2. Fall Für die anderen Summanden ist $hq+r \gg (h+1)q$, da dies für $r > q/2$ stimmt und für $r \le q/2$ und $h \ge 1$ ist $hq+r > hq \ge \frac{(h+1)q}{2} \Leftrightarrow hq \ge q$. Deren Beitrag ist also

$$\ll \sum_{0 \le h < \frac{L}{q}} \sum_{r=1}^{q} \min\Big(\frac{n}{(h+1)q}, \Big\|\frac{ra}{q} + hq\beta + r\beta\Big\|^{-1}\Big).$$

Behauptung: Für ein Intervall $I \subseteq [0,1]$ der Länge $\frac{1}{q}$ gibt es bei festem h zu $t(r) := \Big\|\frac{ra}{q} + hq\beta + r\beta\Big\| \in I$ (d. h. mod 1) höchstens vier Lösungen in $1 \le r \le q$.

⌜

Sei $I = [\gamma, \gamma + 1/q]$, so muß

$$\frac{ra}{q} + hq\beta \in [\gamma - 1/q, \gamma + 2/q]$$

liegen, damit $t(r) \in I$. Denn die $\frac{ra}{q}$ durchlaufen alle Brüche $0/q, 1/q, \ldots, \frac{q-1}{q}$, die Zahl $hq\beta$ ist fest, und es ist $|r\beta| \le 1/q$. Der Abstand dieser Punkte $\frac{ra}{q} + hq\beta$ voneinander ist $\ge 1/q$ für verschiedene r, also liegen höchstens 4 dieser Punkte in $[\gamma - 1/q, \gamma + 2/q]$, also höchstens 4 der $t(r)$ in I.

⌟

Wähle nun $I_s = \left[\frac{s}{q}, \frac{s+1}{q}\right]$ mit $0 \le s \le q-1$. Für $\delta \in I_s,\ s \ge 1$, ist also $\frac{1}{\delta} \ll \frac{q}{s}$, somit ist deren Beitrag

$$\begin{aligned} &\ll \frac{n}{q} + \sum_{1 \le h \le L/q} \frac{n}{hq} + \sum_{0 \le h \le L/q} \sum_{s=1}^{q-1} \sum_{\substack{r, \\ t(r) \in I_s}} \frac{q}{s} \\ &\ll \frac{1}{q} \sum_{h \le L/q} \frac{n}{h} + \sum_{0 \le h < L/q} \sum_{s=1}^{q-1} \frac{q}{s} \ll \frac{n}{q} \log L + \frac{L}{q} \cdot q \log q, \end{aligned}$$

ebenfalls klein genug.

□

§ 3.5. Beweisschluß des Satzes von Vinogradov

(Lösung des ternären Goldbach–Problems für $n \geq n_0, 2 \nmid n$)

Zunächst muß aus Satz 3.5. der Abschätzung von $S(\alpha)$ eine Abschätzung für $\int\limits_{\mathfrak{m}} S^3(\alpha)e(-n\alpha)d\alpha$ gewonnen werden.
Wir haben für $\alpha \in \mathfrak{m}$ ja $(a,q)=1,\ Q \leq q \leq \frac{n}{Q},\ Q=(\log n)^B$ mit $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}$, wie wir nach Satz 3.6. gesehen haben.
Anwendung von Satz 3.5. liefert für $\alpha \in \mathfrak{m}$ also

$$S(\alpha) \ll \Big(\frac{n}{q^{1/2}} + n^{4/5} + (nq)^{\frac{1}{2}}\Big)(\log n)^4$$

also

$$\max_{\alpha\in\mathfrak{m}} \big|S(\alpha)\big| \ll \Big(\frac{n}{Q^{1/2}} + n^{4/5}\Big)(\log n)^4 \ll \frac{n}{(\log n)^{B/2-4}}.$$

Für das $\int\limits_{\mathfrak{m}}$ erhalten wir damit:

$$\begin{aligned}
\Big|\int_{\mathfrak{m}} S^3(\alpha)e(-n\alpha)d\alpha\Big| &\leq \max_{\alpha\in\mathfrak{m}}\big|S(\alpha)\big| \cdot \int_0^1 |S(\alpha)|^2 d\alpha \\
&\ll \frac{n}{(\log n)^{B/2-4}} \cdot n(\log n)^2 \\
&= \frac{n^2}{(\log n)^{B/2-6}} \ll \frac{n^2}{(\log n)^A} \text{ für } B/2-6 \geq A,
\end{aligned}$$

wobei wir

$$\int_0^1 |S(\alpha)|^2 d\alpha = \sum_{p_1,p_2\leq n} \log p_1 \log p_2 \underbrace{\int_0^1 e(\alpha(p_1-p_2))d\alpha}_{=\begin{cases}1, & p_1=p_2\\ 0, & \text{sonst.}\end{cases}} \ll n(\log n)^2$$

abgeschätzt haben. Wir fassen dies zusammen mit Satz 3.3. über die major arcs zu

$$\begin{aligned}
R(n) &= \int_{\mathfrak{M}} S^3(\alpha)e(-n\alpha)d\alpha + \int_{\mathfrak{m}} S^3(\alpha)e(-n\alpha)d\alpha \\
&= \mathcal{S}(n)\cdot\frac{n^2}{2} + \mathrm{O}\Big(\frac{n^2}{(\log n)^A}\Big).
\end{aligned}$$

Aus dieser asymptotischen Formel für $R(n) = \sum\limits_{p_1+p_2+p_3=n} \log p_1 \log p_2 \log p_3$ ist nun die für $r(n) = \sum\limits_{p_2+p_2+p_3=n} 1$ herzuleiten.

- Es ist $R(n) \le r(n)(\log n)^3$.
  $\rightsquigarrow$ also $r(n) > 0$ falls $R(n) > 0$, d. h. damit ist das ternäre Goldbachproblem für große ungerade n, wenn also $\mathcal{S}(n) \gg 1$ gilt, bereits gelöst.
- Sei nun $0 < \delta < \frac{1}{2}$ und $r_\delta(n) := \sum\limits_{\substack{p_1+p_2+p_3=n \\ p_i \le n^{1-\delta} \text{ für ein } i}} 1$

Dann ist

$$r_\delta(n) \le 3 \sum_{\substack{p_1+p_2+p_3=n \\ p_1 \le n^{1-\delta}}} 1 \ll \sum_{p_1 \le n^{1-\delta}} \Big(\sum_{p_2+p_3=n-p_1} 1 \Big) \le \sum_{p_1 \le n^{1-\delta}} \Big(\sum_{p_2<n} 1 \Big)$$
$$\le \pi(n^{1-\delta})\pi(n) \ll \frac{n^{2-\delta}}{(\log n)^2}.$$

Damit erhalten wir

$$\begin{aligned} R(n) &\ge \sum_{\substack{p_1+p_2+p_3=n \\ p_1,p_2,p_3 > n^{1-\delta}}} \log p_1 \log p_2 \log p_3 \ge (1-\delta)^3 (\log n)^3 \sum_{\substack{p_1+p_2+p_3=n \\ p_1,p_2,p_3 > n^{1-\delta}}} 1 \\ &\ge (1-\delta)^3 (\log n)^3 \big(r(n) - r_\delta(n) \big) \\ &\gg (1-\delta)^3 (\log n)^3 \Big(r(n) - \frac{n^{2-\delta}}{(\log n)^2} \Big). \end{aligned}$$

Somit ist

$$(\log n)^3 r(n) \ll \frac{1}{(1-\delta)^3} R(n) + (\log n) n^{2-\delta}.$$

Für $0 < \delta < \frac{1}{2}$ ist $c_2 < 1 - \delta < 1$ und $0 < \frac{1}{(1-\delta)^3} - 1 = \frac{1-(1-\delta)^3}{(1-\delta)^3} \le 8(1-(1-\delta)^3) < 24\delta$.
Wegen der asymptotischen Formel für $R(n)$ ist insbesondere $R(n) \ll n^2$ und somit

$$\begin{aligned} 0 \le (\log n)^3 r(n) - R(n) &\le \Big(\frac{1}{(1-\delta)^3} - 1 \Big) R(n) + (\log n) n^{2-\delta} \\ &\ll \delta\, R(n) + (\log n) n^{2-\delta} \ll \delta\, n^2 + (\log n) n^{2-\delta} = n^2 \Big(\delta + \frac{\log n}{n^\delta} \Big). \end{aligned}$$

Diese Ungleichung gilt für alle $\delta \in \big(0, \frac{1}{2}\big)$, die implizierte Konstante ist unabhängig von δ.
Sei nun $\delta := \frac{2 \log\log n}{\log n}$. Dann ist $\delta + \frac{\log n}{n^\delta} = \frac{2 \log\log n}{\log n} + \frac{\log n}{n^\delta} \ll \frac{\log\log n}{\log n}$ und somit

$$0 \le (\log n)^3 r(n) - R(n) \ll n^2 \cdot \frac{\log\log n}{\log n}.$$

Für $A \ge 1$ folgt mit der asymptotischen Formel für $R(n)$
also

$$(\log n)^3 r(n) = R(n) + \mathrm{O}\Big(n^2 \cdot \frac{\log\log n}{\log n} \Big) = \mathcal{S}(n) \cdot \frac{n^2}{2} + \mathrm{O}\Big(\frac{n^2}{(\log n)^A} \Big) + \mathrm{O}\Big(\frac{n^2 \log\log n}{\log n} \Big)$$

$$= \mathcal{S}(n) \cdot \frac{n^2}{2}\Big(1 + \mathrm{O}\Big(\frac{\log\log n}{\log n}\Big)\Big).$$

also

$$r(n) = \mathcal{S}(n) \cdot \frac{n^2}{2(\log n)^3}\Big(1 + \mathrm{O}\Big(\frac{\log\log n}{\log n}\Big)\Big).$$

Damit ist der Satz von Vinogradov über das ternäre Goldbach–Problem bewiesen. In nächsten § 3.6. machen wir noch einige Bemerkungen zum binären Goldbach–Problem.

§ 3.6. Bemerkung zum binären Goldbach–Problem

Wie beim ternären Problem (dort wurde $\int\limits_{\mathfrak{M}} S^3(\alpha)e(-n\alpha)d\alpha$ ausgewertet)
kann auch

$$\int\limits_{\mathfrak{M}} S^2(\alpha)e(-n\alpha)d\alpha = \mathcal{S}_{(2)}(n) \cdot n + \mathrm{O}\Big(\frac{n}{(\log n)^A}\Big)$$

gezeigt werden, wobei die singuläre Reihe hier

$$\mathcal{S}_{(2)}(n) = \sum_{q=1}^{\infty} \frac{\mu^2(q)}{\varphi^2(q)} c_q(-n) = \prod_{p|n}\Big(1 + \frac{1}{p-1}\Big) \cdot \prod_{p\nmid n}\Big(1 - \frac{1}{(p-1)^2}\Big)$$

ist; und sie ist $\neq 0$ für **gerades n**.
Die Schwierigkeit besteht hier in der Auswertung der minor arcs. Würde man wie oben abschätzen, so schafft man nur

$$\Big|\int\limits_{\mathfrak{m}} S^2(\alpha)e(-n\alpha)d\alpha\Big| \le \underbrace{\max_{\alpha\in\mathfrak{m}}|S(\alpha)|}_{\ll \frac{n}{(\log n)^{c+1}}} \cdot \underbrace{\int\limits_{\mathfrak{m}} |S(\alpha)|d\alpha}_{\ll \left(\int\limits_0^1 |S(\alpha)|^2 d\alpha\right)^{1/2} \ll n^{1/2}(\log n)} \ll \frac{n^{3/2}}{(\log n)^c},$$

gebraucht wird aber eine Abschätzung, die besser als $\ll n$ ist.
Hierfür ist kein Weg in Sicht, auch nicht unter Annahme der GRH. Allerdings schafft man folgende Abschätzung: Es ist

$$\sum_{m=1}^{n} \Big|\int\limits_{\mathfrak{m}} S^2(\alpha)e(-m\alpha)d\alpha\Big|^2 \ll \frac{n^3}{(\log n)^A}.$$

⌜
Es gilt die Besselsche Ungleichung $\sum\limits_{m\le n} |\langle v, e_m\rangle|^2 \le \langle v, v\rangle$ $(=: \|v\|^2)$ für eine Teilfolge (e_m) eines Orthonormalsystems in einem Prähilbertraum, v ein beliebiger Vektor daraus.

Hier auf die linke Seite angewandt zeigt diese, daß diese nach oben abschätzbar ist durch

$$\leq \int\limits_{\mathfrak{m}} \big|S(\alpha)\big|^4 d\alpha \ll \max_{\alpha\in\mathfrak{m}} \big|S(\alpha)\big|^2 \cdot \int\limits_0^1 \big|S(\alpha)\big|^2 d\alpha \ll \frac{n^2}{(\log n)^{A+2}} \cdot n(\log n)^2 = \frac{n^3}{(\log n)^A}$$

⌟

Weiter folgt aus der obigen asymptotischen Formel für $\int\limits_{\mathfrak{M}}$, daß

$$\sum_{m=1}^{n} \Big| \int\limits_{\mathfrak{M}} S^2(\alpha) e(-m\alpha) d\alpha - \mathcal{S}_{(2)}(m) \cdot m \Big|^2 \ll \frac{n^3}{(\log n)^A} \quad \text{gilt.}$$

Somit erhalten wir insgesamt

$$\sum_{m=1}^{n} \Big| \int\limits_{0}^{1} S^2(\alpha) e(-m\alpha) d\alpha - \mathcal{S}_{(2)}(m) \cdot m \Big|^2 \ll \frac{n^3}{(\log n)^A}.$$

Korollar 1. *Sei* $\mathcal{E}(n) := \{m \leq n;\ 2 \mid m\ \&\ m \neq p_1 + p_2\}$ *die Menge der Goldbach–Ausnahmen bis* n*. Dann ist deren Anzahl*

$$\#\,\mathcal{E}(n) \ll \frac{n}{(\log n)^A} \quad \textit{bzw.} \quad \frac{\#\mathcal{E}(n)}{n} \ll \frac{1}{(\log n)^A} \longrightarrow_{n\to\infty} 0.$$

„Fast alle“ geraden $m \leq n$ *erfüllen also die binäre Goldbach–Vermutung.*

Beweis. Für jedes $m \in \mathcal{E}(n)$ gilt $\int\limits_0^1 S^2(\alpha) e(-m\alpha) d\alpha = 0$, also

$$n^2 \cdot \#\,\mathcal{E}'(n) \ll \sum_{\substack{\frac{n}{2} < m \leq n \\ m \in \mathcal{E}(n)}} \underbrace{\Big| \int_0^1 S^2(\alpha) e(-m\alpha) d\alpha - S_{(2)}(m) m \Big|^2}_{\gg m^2 > (n/2)^2} \ll \frac{n^3}{(\log n)^{A+1}},$$

wobei $\mathcal{E}'(n) = \big\{\frac{n}{2} < m \leq n; m \in \mathcal{E}(n)\big\}$ ist, d.h. $\#\,\mathcal{E}'(n) \ll \frac{n}{(\log n)^{A+1}}$. Dann ist

$$\#\,\mathcal{E}(n) \ll \sum_{\substack{k \leq n \\ k = 2^i}} \#\,\mathcal{E}'(k) \ll (\log n) \cdot \max_{\substack{k = 2^i \leq n \\ (n \geq n_0)}} \frac{k}{(\log k)^{A+1}} \ll \frac{n}{(\log n)^A}.$$

Wir hatten bereits in § 3.1. erwähnt, daß neuerdings sogar $\#\,\mathcal{E}(n) \ll n^\vartheta$ mit $\vartheta < \frac{2}{3}$ gezeigt werden kann. □

§ 4 Das Waringsche Problem und der Satz von Waring–Hilbert

§ 4.1. Das Waringsche Problem

Edward Waring behauptete 1770 ohne Angabe eines Beweises, daß jede natürliche Zahl die Summe von 4 Quadraten, 9 Kuben, 19 4–ten Potenzen usw. sei.

Waringsches Problem: $\forall\, k \geq 2\ \exists\, g(k) \in \mathbb{N}\ \forall\, n \in \mathbb{N}:$

$$\exists\, n_1, \ldots, n_\ell \in \mathbb{N}:\ n = n_1^k + \cdots + n_\ell^k,\ 1 \leq \ell \leq g(k),$$

d.h. n läßt sich als Summe von höchstens $g(k)$ vielen k–ten Potenzen natürlicher Zahlen schreiben.

Anders ausgedrückt:
Für jedes $k \geq 2$ ist die Menge der natürlichen k–ten Potenzen eine Basis endlicher Ordnung. Gesucht ist auch die Größe dieser Ordnung, also das **kleinste** $g(k)$, das Warings Behauptung erfüllt. Für $k = 2$ liefert der Satz von Lagrange bzw. Euler den exakten Wert $g(2) = 4$.

Das allgemeine Problem in dem Sinne, daß $g(k) < \infty$ gilt, wurde erst 1909 von David Hilbert gezeigt. 1919 fanden Hardy und Littlewood eine Lösung des Problems mit ihrer Kreismethode, die von ihnen insbesondere für das Waringproblem entwickelt wurde. Die hier ab § 4.2. vorgestellte Lösung geht auf Yuri Linnik zurück und benutzt Ergebnisse von Lew Schnirelman.

Doch bereits die genaue Bestimmung von $g(3)$ ist ein schwieriges Problem, also die Lösung des Waringschen Problems für Kuben.
Wieferich und Kempner zeigten um 1910, daß $g(3) = 9$.
Dies ist optimal, weil sich 23 und 239 **nicht** als Summe von höchstens 8 Kuben schreiben lassen.
Später zeigte Landau um 1926, daß nur endlich viele natürliche Zahlen 9 Kuben benötigen, d. h. jede hinreichend große natürliche Zahl ist Summe von ≤ 8 Kuben.
Sei $G(3)$ die kleinste Zahl, so daß sich jedes hinreichend großes n als Summe von $\leq G(3)$ vielen Kuben schreiben läßt, also

$$\exists\, n_0\ \forall\, n \geq n_0:\ \exists\, n_1, \ldots, n_\ell \in \mathbb{N}:\ n = n_1^3 + \ldots + n_\ell^3 \text{ mit } \ 1 \leq \ell \leq G(3).$$

- Landau zeigte also $G(3) \leq 8$.
- Dickson zeigte 1939, daß 23 und 239 die **einzigen** natürlichen Zahlen sind, die nicht als Summe von ≤ 8 Kuben geschrieben werden können.
- Linnik zeigte, daß $G(3) \leq 7$ (schwer!), es gilt: $4 \leq G(3) \leq 7$. Der exakte Wert von $G(3)$ ist bis heute unbekannt. Die Behauptung $g(4) = 19$ wurde erst 1992 bewiesen.

Über natürliche Zahlen, die Summe von 2 Kuben sind, ist folgendes bekannt:

1. es gibt natürliche Zahlen mit beliebig vielen Darstellungen als Summe von 2 Kuben,
2. für fast alle natürlichen Zahlen, die Summe 2er Kuben sind, ist diese Darstellung eindeutig.

Dazu die folgende Anekdote über Hardy und Ramanujan: Hardy besuchte den schwerkranken Ramanujan im Krankenhaus und berichtete beiläufig, daß er zur Hinfahrt das Taxi mit der Nummer $1729 = 7 \cdot 13 \cdot 19$ benutzt hatte, eine völlig langweilige Zahl. Daraufhin entgegnete ihm Ramanujan, daß 1729 sehr wohl eine interessante Zahl sei, nämlich die kleinste Zahl, die auf 2 Arten als Summe zweier Kuben dargestellt werden kann:

$$1729 = 12^3 + 1^3 = 10^3 + 9^3.$$

Man nennt die kleinste Zahl, die auf k Arten als Summe von 2 Kuben geschrieben werden kann, daher die k-te Taxizahl.

§ 4.2. Der Satz von Schnirelman

Zur Vorbereitung des Satzes von Hilbert-Waring, nämlich

Satz 4.1. *Für alle $k \geq 2$ ist $g(k) < \infty$,*

benötigen wir Ergebnisse von Schnirelman, die wir in diesem § entwickeln.

Definition 4.2. (Basis, Ordnung): Seien $\mathcal{A}, \mathcal{B} \subseteq \mathbb{N}_0$.

1.) $\mathcal{A} + \mathcal{B} := \{c \in \mathbb{N}_0;\ \exists\, a \in \mathcal{A}\ \exists\, b \in \mathcal{B} : c = a + b\}$ heißt die **Summe** der Mengen $\mathcal{A}$ und $\mathcal{B}$.

2.) $n\mathcal{A} := \{c \in \mathbb{N}_0;\ \exists\, a_1, \ldots, a_n \in \mathcal{A} : c = a_1 + \cdots + a_n\} = \underbrace{\mathcal{A} + \mathcal{A} + \cdots + \mathcal{A}}_{n \text{ mal}}$

3.) $\mathcal{A}$ heißt **Basis** (von $\mathbb{N}$), wenn es ein $n \in \mathbb{N}$ gibt mit $n\mathcal{A} \supseteq \mathbb{N}$ (also „$=$“, d. h. $\mathcal{A}$ ist Basis bezüglich n). Das kleinste solche n heißt **Ordnung** der Basis.

4.) $A(n) := \#\{1 \leq a \leq n;\ a \in \mathcal{A}\}$ **Zählfunktion** von $\mathcal{A}$

5.) $\sigma(\mathcal{A}) := \inf\limits_{n \in \mathbb{N}_{(\geq 1)}} \frac{A(n)}{n}$ **Schnirelman–Dichte** von $\mathcal{A}$. $\Big[$ **Bem.** inf, **nicht** lim inf!$\Big]$

6.) $\mathcal{A}$ hat **positive Dichte**, wenn $\sigma(\mathcal{A}) > 0$ ist.

Folgerung 4.3. *1.)* $0 \leq \sigma(\mathcal{A}) \leq 1$

2.) $\mathcal{A}$ hat positive Dichte $\Leftrightarrow \exists\, \alpha > 0\, \forall\, n \in \mathbb{N} : A(n) \geq \alpha n$.

3.) $1 \notin \mathcal{A} \Rightarrow \sigma(\mathcal{A}) = 0$ $\quad \lceil$ *da* $A(1) = 0 \rfloor$
$n \notin \mathcal{A} \Rightarrow \sigma(\mathcal{A}) \leq \frac{n-1}{n}$ $\quad \lceil$ *da* $A(n) \leq n - 1 \rfloor$

Hilfssatz 4.4. *Sei* $mA, \mathcal{B} \subseteq \mathbb{N}_0,\ 1 \in \mathcal{A},\ 0 \in \mathcal{B}$.
Dann: $\sigma(\mathcal{A}+\mathcal{B}) \geq \sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\sigma(\mathcal{B})$.

Beweis. Sei $n \in \mathbb{N}$ und seien $1 = a_1 < a_2 a \ldots a_r \leq n$ die Elemente von $\mathcal{A} \cap \{1, \ldots, n\}$ $\rightsquigarrow$ $r = A(n)$.
Für $1 \leq j \leq r$ sei

$$g_j = \begin{cases} a_{j+1} - a_j - 1, & 1 \leq j \leq r-1 \\ n - a_r, & j = r \end{cases}$$

$\Rightarrow$ In jedem IV $[a_j, a_j + 1)$ bzw. $[a_r, n]$ sind $\geq B(g_j) + 1$ viel Elemente von $\mathcal{A}+\mathcal{B}$, nämlich $a_j = a_j + 0$, und die $a_j + b_\ell$ mit $1 \leq b_\ell \leq g_j$.

$$\Rightarrow \quad \underbrace{(A+B)(n)}_{\text{(Zählfunktion von } \mathcal{A}+\mathcal{B})} \geq r + \sum_{j=1}^{r} B(g_j) \leq A(n) + \sigma(\mathcal{B}) \sum_{j=1}^{r} g_j$$

$$\begin{aligned} &= A(n) + \sigma(\mathcal{B})(n - A(n)) \\ &= \underbrace{A(n)}_{\geq n\sigma(\mathcal{A})} \underbrace{(1 - \sigma(\mathcal{B}))}_{\geq 0} + n\sigma(\mathcal{B}) \\ &\geq n\sigma(\mathcal{A})(1 - \sigma(\mathcal{B})) + n\sigma(\mathcal{B}). \\ \Rightarrow \frac{(A+B)(n)}{n} &\geq \sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\,\sigma(\mathcal{B}). \end{aligned}$$

□

Bem.: Mit größerem Aufwand kann dies verschärft werden zu:

$$0 \in \mathcal{A} \cap \mathcal{B} \Rightarrow \sigma(\mathcal{A}+\mathcal{B}) \geq \min\big\{1,\, \sigma(\mathcal{A}) + \sigma(\mathcal{B})\big\}. \quad \text{(Satz von Mann)}$$

Hilfssatz 4.5. $0, 1 \in \mathcal{A} \Rightarrow \sigma(n\mathcal{A}) \geq 1 - \big(1 - \sigma(\mathcal{A})\big)^n$.

Beweis. VI nach n : $\underline{n = 1 : \checkmark}, \underline{n \rightsquigarrow n+1 :}$ Sei $\sigma := \sigma(\mathcal{A})$. Dann:

$$\begin{aligned} \sigma\big((n+1)\mathcal{A}\big) &\geq \sigma + \sigma(n\mathcal{A}) - \sigma \cdot \sigma(n\mathcal{A}) \geq \sigma + (1-\sigma)\big(1 - (1-\sigma)^n\big) \\ &= \sigma + 1 - (1-\sigma)^n - \sigma + \sigma(1-\sigma)^n = 1 - (1-\sigma)^{n+1}. \end{aligned}$$

□

Damit kann nun gezeigt werden:

Satz 4.6. (Satz von Schnirelman) *Sei* $\mathcal{A} \subseteq \mathbb{N}_0,\ 0 \in \mathcal{A}, \sigma(\mathcal{A}) > 0$.
Dann ist $\mathcal{A}$ *Basis, d.h.* $\exists\, n : n\mathcal{A} = \mathbb{N}_0$.
Eine Menge natürlicher Zahlen positiver (Schnirelman–)Dichte ist eine Basis.

Beweis. Da $\sigma := \sigma(\mathcal{A}) > 0$ ist $1 \in \mathcal{A}$.
4.5. $\rightsquigarrow \exists k \in \mathbb{N} :\ \sigma(k\mathcal{A}) \geq \frac{1}{2}$. (*)
Wir zeigen $2k\mathcal{A} = \mathbb{N}_0$: **Ann.** $\exists m \in \mathbb{N},\ m > 1 :\ m \notin 2k\mathcal{A} = k\mathcal{A} + k\mathcal{A}$
Da $0 \in k\mathcal{A}$ folgt $m \notin k\mathcal{A}$.
Dann

$$\begin{aligned} m &\overset{(*)}{\leq} m \cdot \big(\sigma(k\mathcal{A}) + \sigma(k\mathcal{A})\big) \leq (kA)(m) + (kA)(m) \\ &= (kA)(m-1) + (kA)(m-1), \end{aligned}$$

da $m \notin \mathcal{A}$. Seien

$$\begin{aligned} &1 \leq b_1 < \cdots < b_r \leq m-1 \text{ die Elemente von } k\mathcal{A} \cap \{1, \ldots, m-1\} \\ &\rightsquigarrow r = (ka)(m-1),\ m \leq 2r. \end{aligned}$$

Wir haben $b_1, \ldots, b_r,\ m - b_1, \ldots, m - b_r \in \{1, \ldots, m-1\}$, und wegen $2r \geq m > m-1$ sind mindestens zwei der Zahlen gleich (Schubfachprinzip), also existiert $1 \leq j, \ell \leq r$ mit $b_j = m - b_\ell$, also ist $m = b_j + b_\ell \in 2k\mathcal{A}$, $\lightning$. □

Das Waringsche Problem – ob für $k \geq 2$ die Menge $\mathcal{P}_k = \{0, 1^k, 2^k, 3^k, \ldots\}$ der k–ten Potenzen eine Basis ist – läßt sich mit dem Schnirelmanschen Satz **nicht** auf Anhieb lösen, da $\mathcal{P}_k(m) \leq m^{1/k}$, also $\sigma(\mathcal{P}_k) = 0$ ist.
Unsere Beweisstrategie ist die folgende: Wir zeigen:

$$\oplus \qquad \exists\, L = L(k) :\ \sigma(L\mathcal{P}_k) > 0 \text{ (die Hauptschwierigkeit!)}$$

damit und dem Satz 4.6. von Schnirelman folgt die Behauptung.
Im nächsten § zeigen wir einen Hilfssatz von Linnik, der zum Beweis von $\oplus$ dient.

§ 4.3. Die Linniksche Ungleichung

Wir brauchen zunächst eine obere Abschätzung der Anzahl Lösungen von $x_1y_1 + x_2y_2 = a$ in ganzen Zahlen $|x_j| \leq A$, $|y_j| \leq B$:

Hilfssatz 4.7. *Für $a \in \mathbb{Z},\ A, B \geq 1$ sei*

$$Q(a) = Q(a; A, B) = \#\big\{(x_1, x_2, y_1, y_2) \in \mathbb{Z}^4; \underbrace{x_1y_1 + x_2y_2 = a,}_{\otimes}\ |x_j| \leq A,\ |y_j| \leq B\big\}.$$

Dann ist

$$Q(a) \leq \begin{cases} 27A^{3/2}B^{3/2} + 9A^2 + 9B^2, & \textit{falls} \quad a = 0, \\ 60AB \sum\limits_{d|a} \frac{1}{d}, & \textit{falls} \quad a \neq 0. \end{cases}$$

Beweis.

1. Fall: $a = 0$: Sei zunächst $x_1 = x_2 = 0$, dann ist die Anzahl der möglichen Paare y_1, y_2 dann $(2B+1)^2 = 4B^2 + 4B + 1 \le 9B^2$.

Die Anzahl der Quadrupel mit $y_1 = y_2 = 0$ ist analog $\le 9A^2$.

Zu einem Tripel (x_1, x_2, y_1) mit $x_1 \neq 0$ oder $x_2 \neq 0$ existiert nun höchstens ein y_2 mit $\otimes$, und auch zu (x_1, y_1, y_2) mit $y_1 \neq 0$ oder $y_2 \neq 0$ existiert höchstens ein x_2 mit $\otimes$, die Anzahl solcher Lösungsquadrupel ist somit

$$\begin{aligned}
&\le \min\left\{(2A+1)^2(2B+1),\ (2A+1)(2B+1)^2\right\} \\
&\le 27\min\{A^2B, AB^2\} \\
&\le 27(A^2B \cdot AB^2)^{1/2} \\
&= 27A^{3/2}B^{3/2}
\end{aligned}$$

2. Fall: $a \neq 0, \text{Œ}A \le B$
[durch Vertauschen der Rollen von A und B ist der Fall $B \le A$ analog].

Sei $Q_1(a) = Q_1(a; A, B) := \#\left\{(x_1, x_2, y_1, y_2) \in \mathbb{Z}^4; \otimes,\ (x_1, x_2) = 1,\right.$
$\left.|x_2| \le |x_1| \le A,\ |y_j| \le B\right\}$, [hier ist $x_1 = 0$ ausgeschlossen]
und für $(x_1, x_2) = 1,\ |x_2| \le |x_1| \le A$ sei $Q_2(a, x_1, x_2) := \#\left\{(y_1, y_2), \otimes,\ |y_j| \le B\right\}$.
[für $(x_1, x_2) = 1$ ist $\otimes$ lösbar wegen ggT–Darstellung (Euklidscher Algorithmus).]

Ist (y_{10}, y_{20}) ein Lösungspaar zu $(x_1, x_2) = 1$, so werden alle Lösungen durch $y_1 = y_{10} + bx_2, y_2 = y_{20} - bx_1$ $(b \in \mathbb{Z})$ beschrieben.

Die Beschränkung $|y_1|, |y_2| \le B$ ergibt $|b| = \dfrac{|y_{20} - y_2|}{|y_1|} \le \dfrac{2B}{|x_1|}$, d.h. für b (und damit y_1, y_2) stehen

$$2 \cdot \frac{2B}{|x_1|} + \underbrace{1}_{\substack{\le \frac{B}{|x_1|} \\ \text{da } |x_1| \le A \le B}} \le \frac{5B}{|x_1|}$$

viele Werte zur Verfügung.
Somit ist

$$\begin{aligned}
Q_1(a) &= \sum_{x_1, 1 \le |x_1| \le A} \ \sum_{\substack{x_2, |x_2| \le |x_1| \\ (x_2, x_1) = 1}} Q_2(a, x_1, x_2) \le \sum_{1 \le |x_1| \le A} \ \sum_{|x_2| \le |x_1|} \frac{5B}{|x_1|} \\
&= 5B \sum_{1 \le |x_1| \le A} \underbrace{\frac{2|x_1| + 1}{|x_1|}}_{\le 3} \le 30AB.
\end{aligned}$$

Läßt man die Bedingung $|x_2| \le |x_1|$ in der Definition von $Q_1(a)$ weg, verdoppelt sich die Anzahl höchstens, d. h.

$$\Rightarrow \#\left\{(x_1, x_2, y_1, y_2) \in \mathbb{Z}^4; (x_1, x_2) = 1, \otimes,\ |x_j| \le A,\ |y_j| \le B\right\} \le 60AB.$$

Somit ist die Abschätzung der Behauptung für die Quadrupel mit $(x_1, x_2) = 1$ gezeigt. Falls $(x_1, x_2) =: d$, ist $\otimes$ äquivalent zu

$$x_1' y_1 + x_2' y_2 = \frac{a}{d},\ \text{wo}\ (x_1', x_2') = 1,\ |x_1'| \le \frac{A}{d},\ |y_j| \le B,$$

deren Lösungsanzahl ist also $\le 60 \cdot \dfrac{A}{d} \cdot B$ nach obigen $\Big[\dfrac{A}{d} \le A \le B\Big]$. Also ist

$$Q(a) = \sum_{d|a} Q_1\Big(\frac{a}{d}; \frac{A}{d}, B\Big) \le 60AB \sum_{d|a} \frac{1}{d}.$$

□

Hilfssatz 4.8. (Linniksche Ungleichung)
Sei $A \ge 1,\ k \ge 2,\ C_1 \ge 1$, *und*

$$A(x) = a_k\, x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

ein Polynom mit

$$0 < |a_k| \le C_1,\ |a_{k-1}| \le C_1 A, \ldots, |a_1| \le C_1 A^{k-1},\ |a_0| \le C_1 A^k.$$

Sei I *ein Teilintervall von* $[0, A]$, *und*

$$\mathcal{J}_k = \mathcal{J}_k(C_1, A, f, I) := \int_0^1 \Big| \sum_{x \in I \cap \mathbb{Z}} e\big(\alpha f(x)\big)\Big|^{8^{k-1}} d\alpha.$$

dann ist $\mathcal{J}_k = \mathrm{O}(A^{8^{k-1}-k})$.
Die O*–Konstante hängt von* C_1 *und* k *ab (im Prinzip effektiv berechenbar).*

Bem.

1. Der Beweis wird induktiv nach k geführt, die Bedingung an f ist dabei günstig. Anwenden werden wir Linniks Ungleichung nur für $f(x) = x^k,\ I = [0, A]$.

2. Die triviale Abschätzung ist $\mathcal{J}_k = \mathrm{O}(A^{8^{k-1}})$, d. h. k A–Potenzen werden gewonnen.

Beweis.
1. Induktionsanfang $k = 2$ (d. h. $\deg f = 2$).
Es ist

$$\mathcal{J}_2 = \sum_{\substack{x_1 \ldots x_4 \\ y_1 \ldots y_4 \\ \in I \cap \mathbb{Z}}} \int_0^1 e\big(\alpha(f(x_1) + f(x_2) - f(y_1) - f(y_2) - f(x_3) - f(x_4) + f(y_3) + f(y_4)\big) d\alpha$$

$$\le \#\big\{(x_1 \ldots x_4, y_1 \ldots y_4),\ 0 \le x_j, y_j \le A,\ f(x_1) - f(y_1) + f(x_2) - f(y_2)$$

$$= f(x_3) - f(y_3) + f(x_4) - f(y_4)\big\}.$$

Sei $x'_j := x_j - y_j,\ y'_j := a_2(x_j + y_j) + a_1$. $\lceil a_1, a_2$ Koeffizienten von $f\rfloor$
Dann:

$$f(x_j) - f(y_j) = a_2(x_j^2 - y_j^2) + a_1(x_j - y_j) = x'_j y'_j.$$

Da $0 \le x_j, y_j \le A,\ |a_1| \le C_1 A,\ |a_2| \le C_1$ folgt $|x'_j| \le A,\ |y'_j| \le 3C_1 A$.
Jedem Paar (x'_j, y'_j) mit $|x'_j| \le A,\ |y'_j| \le 3C_1 A$ entspricht (da $a_2 \neq 0$) höchstens 1 Paar (x_j, y_j) mit $0 \le x_j, y_j \le A$.
Also folgt

$$\mathcal{J}_2 \le \#\big\{(x'_1 \dots x'_4, y'_1 \dots y'_4);\ |x_j| \le A,\ |y'_j| \le 3C_1 A, x'_1 y'_1 + x'_2 y'_2 = x'_3 y'_3 + x'_4 y'_4\big\}.$$

Mit Hilfssatz 4.7. folgt

$$\mathcal{J}_2 \le \sum_{|a| \le 6C_1 A^2} Q^2(a, A, 3C_1 A) = \mathrm{O}\Big(A^6 + \sum_{0 < |a| \le 6C_1 A^2} A^4 \Big(\sum_{d|a} \frac{1}{d}\Big)^2\Big).$$

Mit $B := 6C_1 A^2$ ist die $\sum$ über a nun

$$\le 2 \sum_{m \le B} \sum_{d_1 | m} \frac{1}{d_1} \sum_{d_2 | m} \frac{1}{d_2} = 2 \sum_{d_1, d_2 \le B} \frac{1}{d_1 d_2} \underbrace{\sum_{\substack{m \le B \\ m \equiv 0 \ ([d_1, d_2])}} 1}_{\le \frac{B}{[d_1, d_2]}} \le 2B \sum_{d_1, d_2 \le B} \frac{(d_1, d_2)}{d_1^2 d_2^2}$$

$$\le 2B \sum_{d_1, d_2 \le B} \frac{1}{(d_1 d_2)^{3/2}} = \mathrm{O}(B) = \mathrm{O}(A^2),$$

wobei $(d_1, d_2) \le \min\{d_1, d_2\} \le \sqrt{d_1 d_2}$ benutzt wurde. Also folgt:

$$\mathcal{J}_2 = \mathrm{O}(A^6) = \mathrm{O}(A^{8^{2-1}-2}).$$

Die O–Konstante hängt allein von C_1 ab.

2. Induktionsschritt $k > 2$:
Ind.Vor.: Die Ungleichung sei für $k-1$ und alle zulässigen Polynome g vom Grad $k-1$ bewiesen, d. h. die Vor. sei mit einem $C_2 = C_2(C_1, k)$ erfüllt.
2.1. Sei f ein zulässiges Polynom, deg $f = k$
Für $0 \le \alpha \le 1$ gilt dann

$$\Big|\sum_{x \in I \cap \mathbb{Z}} e\big(\alpha f(x)\big)\Big|^2 = \sum_{x, y \in I \cap \mathbb{Z}} e\big(\alpha\big(f(y) - f(x)\big)\big)$$

$$\le \underbrace{A+1}_{\text{Terme mit } y=x} + \sum_{0 < |b| \le A} \underbrace{\sum_{\substack{x \in I \cap \mathbb{Z} \\ x+b \in I \cap \mathbb{Z}}}}_{\Leftrightarrow : x \in I(b)} e\big(\alpha\big(f(x+b) - f(x)\big)\big).$$

Für $0 < |b| \le A$ sei

$$g(x) = g(x,b) := \frac{1}{b}\big(f(x+b) - f(x)\big) = a_k \cdot \frac{1}{b}\big((x+b)^k - x^k\big) + \cdots + a_1 \cdot \frac{1}{b}\big((x+b) - x\big)$$
$$= a_k \cdot \left(\binom{k}{1}x^{k-1} + \binom{k}{2}x^{k-2}b + \cdots + b^{k-1}\right) + \cdots + a_1$$
$$=: \tilde{a}_{k-1}x^{k-1} + \tilde{a}_{k-2}(b)x^{k-2} + \ldots + \tilde{a}_0(b), \quad \text{wobei } \tilde{a}_{k-1} = ka_k \text{ nicht von } b \text{ abhängt.}$$

Es gilt mit $0 < |b| \le A$ dann

$$\tilde{a}_{k-1} = ka_k \neq 0,\ |\tilde{a}_{k-1}| \le C_2,\ |\tilde{a}_{k-2}| \le C_2A, \ldots, |\tilde{a}_0| \le C_2A^{k-1},$$

die Konstante $C_2 = C_2(C_1, k)$ ist mit diesen Ungleichungen festgelegt!
(Beachte, daß die $|a_j| \le C_1A^{k-j}$.)

Die $f(x,b)$ sind also zulässige Polynome, auf die die Induktionsannahme anwendbar ist.
Für $0 = |b| \le A$ setzen wir nun

$$S(b,\alpha) := \sum_{x \in I(b)} e\big(\alpha b g(x,b)\big),$$

und es ist

$$\Big|\sum_{x \in I \cap \mathbb{Z}} e\big(\alpha f(x)\big)\Big|^{2\cdot 8^{k-2}} \le 2^{8^{k-2}} \max\Big\{(A+1)^{8^{k-2}}, \Big|\sum_{0<|b|\le A} S(b,\alpha)\Big|^{8^{k-2}}\Big\} \qquad (\otimes)$$

2.2. Die Höldersche Ungleichung

$$\Big(\sum_v \alpha_v\beta_v\Big)^c \le \Big(\sum_v \alpha_v^{c'}\Big)^{c/c'}\Big(\sum_v b_v^c\Big)$$

$\lceil$die $\alpha_v, \beta_v \ge 0,\ c, c' > 0,\ \dfrac{1}{c} + \dfrac{1}{c'} = 1$, d.h. $\dfrac{c}{c'} = c - 1 > 0\rfloor$
mit $c := 8^{k-2}$ liefert

$$\Big|\sum_{0<|b|\le A} 1 \cdot S(b,a)\Big|^{8^{k-2}} \le (2A)^{8^{k-2}-1} \sum_{0<|b|\le A} \big|S(b,a)\big|^{8^{k-2}},$$

und es folgt

$$\Big|\sum_{x\in I} e\big(\alpha f(x)\big)\Big|^{2\cdot 8^{k-2}} = \mathrm{O}_{(k)}\Big(\max\Big\{A^{8^{k-2}}, A^{8^{k-2}-1}\sum_{0<|b|\le A}\big|S(b,\alpha)\big|^{8^{k-2}}\Big\}\Big).$$

2.3. Für $0 < |b| \le A$ sei

$$\big|S(b,a)\big|^{8^{k-2}} = \Big|\sum_{x\in I(b)} e\big(\alpha b\, g(x)\big)\Big|^{8^{k-2}}$$

$$=: \sum_y T(y,b)e(\alpha by),$$

wobei $T(y,b) \neq 0$ nur für

$$|y| \leq 8^{k-2} \max_{x \in I(b)} \big|g(x,b)\big| = \mathrm{O}(A^{k-1})$$

möglich ist.

$$\begin{aligned}
\Rightarrow \big|T(y,b)\big| &= \Big| \int_0^1 \Big(\sum_{y'} T(y',b)e(\alpha by')\Big) e(-\alpha by) d\alpha \Big| \\
&= \Big| \int_0^1 \Big| \sum_{x \in I(b)} e\underbrace{(\alpha b}_{\rightsquigarrow \beta} g(x,b))\Big|^{8^{k-2}} e(-\underbrace{\alpha b}_{\rightsquigarrow \beta} y) d\alpha \Big| \\
&= \Big| \frac{1}{b} \int_0^b \Big| \sum_{x \in I(b)} e\big(\beta g(x,b)\big)\Big|^{8^{k-2}} e(-\beta y) d\beta \Big| \\
&= \Big| \int_0^1 \Big| \sum_{x \in I(b)} e\big(\alpha g(x,b)\big)\Big|^{8^{k-2}} e(-\alpha y) d\alpha \Big| \\
&\leq \int_0^1 \Big| \sum_{x \in I(b)} e\big(\alpha g(x,b)\big)\Big|^{8^{k-2}} d\alpha.
\end{aligned}$$

Auf dieses $\int_0^1$ wenden wir die Induktion vor. an, es folgt $T(y,b) = \mathrm{O}\big(A^{8^{k-2}-(k-1)}\big)$.

2.4. Somit:

$$\begin{aligned}
\mathcal{J}_k &= \mathrm{O}\Big(\int_0^1 \big(A^{4\cdot 8^{k-2}} + A^{4\cdot 8^{k-2}-4} \Big(\sum_{0<|b|\leq A} \big|S(b,\alpha)\big|^{8^{k-2}}\Big)^4\big) d\alpha\Big) \\
&= \mathrm{O}\big(A^{4\cdot 8^{k-2}}\big) + \mathrm{O}\big(A^{4\cdot 8^{k-2}-4} \int_0^1 \Big(\sum_{0<|b|\leq A} T(y,b)e(\alpha by)\Big)^4 d\alpha\big).
\end{aligned}$$

Das $\int_0^1 ()^4$ ist nun

$$\overset{\mathrm{ONR}}{=} \sum_{\substack{0<|b_1|,\ldots,|b_4|\leq A \\ y_1b_1+\cdots+y_4b_4=0}} \sum_{|y_j|\leq C_3A^{k-1}} T(y_1,b_1)\cdots T(y_4,b_4).$$

Mit $y_3 \rightsquigarrow -z_3$, $y_4 \rightsquigarrow -z_4$ und der Abschätzung für die $T(y,b)$ ist dies

$$= \mathrm{O}\Big(A^{4\cdot 8^{k-2}-4(k-1)} \# \big\{(b_1 \ldots b_4,\, y_1, y_2, z_1, z_2);\ 0 < |b_j| \leq A,$$

$$|y_j|, |z_j| \le C_3 A^{k-1},\ b_1 y_1 + b_2 y_2 = b_3 z_3 + b_4 z_4\big\}\Big).$$

Wie bei $k = 2$ läßt sich die 8–Tupel–Anzahl mit HS 4.7 abschätzen zu

$$\le \sum_{|a|\le 2C_3A^k} Q^2(a; A, C_3A^{k-1}) = \mathrm{O}\Big(A^3 \cdot A^{3(k-1)} + \sum_{0<|a|\le 2C_3A^k} A^2 \cdot A^{2(k-1)} \Big(\sum_{d|a} \frac{1}{d}\Big)^2\Big)$$
$$= \mathrm{O}(A^{3k})$$

Zusammenfassung:

$$\mathcal{J}_k = \mathrm{O}(A^{4\cdot 8^{k-2}}) + \mathrm{O}(A^{4\cdot 8^{k-2}-4+4\cdot 8^{k-2}-4k+4+3k}) = \mathrm{O}(A^{4\cdot 8^{k-2}}) + \mathrm{O}(A^{8^{k-1}-k}) = \mathrm{O}(A^{8^{k-1}-k}).$$

□

§ 4.4. Der Satz von Waring–Hilbert

Jetzt sind wir in der Lage, zu zeigen:

Satz 4.9. (Satz von Waring–Hilbert): *Zu jedem $k \ge 2$ existiert ein $g(k) \in \mathbb{N}$, so daß jedes $n \in \mathbb{N}$ in der Form $n = n_1^k + \ldots x_{g(k)}^k$ (die $x_j \in \mathbb{N}_0$) darstellbar ist.* [$\Leftrightarrow$ „$g(k) < \infty$“]

Beweis.
1. Sei

$$L := \frac{1}{2} \cdot 8^{k-1},\ \mathcal{R}(n) := \#\big\{(x_1, \ldots, x_L) \in \mathbb{N}_0^L; x_1^k + \cdots + x_L^k = n\big\}.$$

Für $N \ge 2L$ gilt:

$$\sum_{n\le N} \mathcal{R}(n) = \sum_{0\le a\le N} \#\big\{(x_1, \ldots, x_L) \in \mathbb{N}_0^L; x_L^k = a\big\} \underbrace{-1}_{\text{für Extraterm } a=0}$$
$$\ge (\#\{0 \le x \le \big(\frac{N}{L}\big)^{\frac{1}{k}}\})^L - 1$$
$$\ge \Big(\frac{N}{L}\Big)^{L/k} - 1 \overset{N>L}{\ge} C_5 N^{L/k}$$

Da $\mathcal{R}(n) \ge 1$ gilt diese Abschätzung für alle $N \ge 1$ mit einem $C_4 \in (0, C_5]$.
⌈ Für $N \in [1, 2L]$ ist $\sum\limits_{n\le N} \mathcal{R}(n) \ge 1 \ge N^{L/k}(2L)^{-L/k}$, also $C_4 = \min\big\{C_5, (2L)^{-L/k}\big\}$ tut's ⌋

2. Für alle $N \ge 1$ gilt

$$\sum_{n\le N} \mathcal{R}^2(n) \le C_6 N^{2L/k-1}.$$

⌈ $A := \lfloor N^{1/k} \rfloor$, für $N \ge C_7$ ist $M := LA^k \ge N$, da $L \ge 4$. Somit:

$$\sum_{n\le N} \mathcal{R}^2(n) \le \sum_{0\le a\le M} \Big(\#\big\{(x_1, \ldots, x_L);\ 0 \le x_j \le A,\ x_1^k + \cdots + x_L^k = a\big\}\Big)^2$$

$$\overset{\text{ONR}}{=} \int_0^1 \Big| \sum_{0\le a\le M} e(\alpha a)\#\big\{(x_1,\dots,x_L);\ 0\le x_j\le A,\ x_1^k+\dots+x_L^k=a\big\}\Big|^2 d\alpha$$

$$= \int_0^1 \Big| \sum_{0\le x_1,\dots,x_L\le A} e\big(\alpha(x_1^k+\dots+x_L^k)\big)\Big|^2 d\alpha = \int_0^1 \Big| \sum_{0\le x\le A} e(\alpha x^k)\Big|^{2L} d\alpha.$$

Das $\int_0^1$ ist nach HS 4.8. $= \mathrm{O}(A^{8^{k-1}-k}) = \mathrm{O}(N^{2L/k-1})$.
Für alle $N \ge 1$ gilt dies, wenn man die O–Konstante ev. vergrößert.

3. Die CS–Ungleichung ergibt

$$\Big(\sum_{n\le N} 1\cdot\mathcal{R}(n)\Big)^2 \le \Big(\sum_{\substack{n\le N\\ \mathcal{R}(n)>0}} 1\Big)\Big(\sum_{n\le N}\mathcal{R}^2(n)\Big),\ \text{mit Schritt 1.\,\&\,2. folgt also}$$

$$\sum_{\substack{n\le N\\ \mathcal{R}(n)>0}} 1 \ge C_8 N^{2L/k-2L/k+1} = C_8\cdot N.$$

Somit hat die Menge

$$\mathcal{A} := \big\{n; \mathcal{R}(n)>0\big\} = \{n;\ n \text{ ist Summe von } L \text{ vielen } k\text{–ten Potenzen}\}$$

positive Dichte, da $\forall\, N\ge 1 : \dfrac{A(N)}{N} = \dfrac{\#\{n\le N; \mathcal{R}(n)>0\}}{N} \ge C_8 > 0.$
Nach dem Satz 4.6 von Schnirelman folgt, daß die Menge $\mathcal{A}\cup\{0\}$ eine Basis ist (etwa von Ordnung $\tilde g(k)$), d.h. jedes $n\in\mathbb{N}$ läßt sich als Summe von $\tilde g(k)$ vielen Elementen von $\mathcal{A}$ schreiben, die selbst wiederum Summe von $\le L$ vielen k–ten Potenzen ist. Dies zeigt Satz 4.9 mit einem $g(k)\le L\tilde g(k)$. □

1. Bem.: Der Linnikschе Beweis mit der Linnikschen Ungleichung, die die obere Schranke für $\sum_{n\le N}\mathcal{R}^2(n)$ liefert, reicht gerade haarscharf aus, um positive Schnirelman-Dichte für $\mathcal{A}$ zu zeigen. Eine schwächere Ungleichung reicht nicht.

2. Bem.: Der Beweis würde zwar eine obere Abschätzung für $g(k)$ liefern; diese wäre allerdings astronomisch hoch und nicht lohnend. Genaueres liefert die Linnik-Methode nicht. Besseres liefert hingegen die Hardy–Littlewoodsche Kreismethode für

$$G(k) = \min\big\{\ell;\ \exists\, N_0\ \forall\, n\ge N_0\ \exists\, x_1,\dots,x_\ell\in\mathbb{N}_0 : n = x_1^k+\dots+x_\ell^k\big\},$$

nämlich $G(k)\le \log k\cdot\big(k+\mathrm{o}(1)\big),\ (k\to\infty)$.

3. Bem.: Stets gilt $G(k)\le g(k)$. In einer Übung wird $G(k)\ge k+1$ gezeigt.

§ 5 Selbergsche Siebtheorie und additive Primzahltheorie

§ 5.1. Das Selbergsche Sieb und zwei Anwendungen

In diesen §en geben wir einen Einblick in die Siebtheorie. Die moderne Siebtheorie ist mittlerweile ein mächtiges Hilfsmittel in der Mathematik, nicht nur in der Zahlentheorie, woher sie ursprünglich kommt. Das einfachste und älteste Sieb – das Sieb des Eratosthenes – dient dem Aufspüren aller Primzahlen $\leq n$ mittels einem einfachen „Siebprozeß“: Ist eine Tabelle mit allen Primzahlen $p \leq \sqrt{x}$ bekannt, so sind aus einer Tabelle mit allen ganzen Zahlen $\in (\sqrt{x}, x]$ diejenigen zu streichen (zu „sieben“), die Vielfache einer Primzahl $p \leq \sqrt{x}$ sind; die übrigen Zahlen im Intervall $(\sqrt{x}, x]$, die also nicht „durch das Sieb gefallen sind“, sind dann genau die Primzahlen $\in (\sqrt{x}, x]$. Dieses Sieb beruht auf der einfachen Beobachtung, daß eine zusammengesetzte Zahl n einen Primteiler $\leq \sqrt{n}$ hat und ist für nicht zu große x sehr gut praktisch anwendbar, um Primzahltabellen zu erstellen oder einen Primzahltest durchzuführen.
Diese Idee eines Siebs wollen wir nun folgendermaßen formalisieren: Sei eine endliche Menge $\mathcal{A} \subseteq \mathbb{N}$ gegeben, und $\mathcal{P}$ eine (beliebige) Menge von Primzahlen, d. h. $\mathcal{P} \subseteq \mathbb{P}$.
Für reelles $z \geq 2$ sei $P(z) := \prod_{\substack{p<z \\ p\in\mathcal{P}}} p$.

Dazu sei die **Siebfunktion** $S(\mathcal{A}, \mathcal{P}, z)$ gegeben durch

$$S(\mathcal{A}, \mathcal{P}, z) := \#\left\{a \in \mathcal{A}; \forall\, p \in \mathcal{P}, p < z : p \nmid a\right\} = \#\left\{a \in \mathcal{A}; \big(a, P(z)\big) = 1\right\}.$$

Die Menge $\{a \in \mathcal{A}; \forall\, p \in \mathcal{P}, p < z : p + a\}$ heißt auch die **gesiebte Menge**, deren Komplement in $\mathcal{A}$ die **ungesiebte Menge**. Im Beispiel des Eratosthenes–Siebs erhält man hier mit $z = \sqrt{x},\ \mathcal{A} = \mathbb{Z} \cap (\sqrt{x}, x]$, als gesiebte Menge gerade die der Primzahlen $\in (\sqrt{x}, x]$. Als anderes Beispiel können wir damit die Primzahlzwillinge (p mit $p + 2$ prim) sieben: Setze $\mathcal{A} := \left\{n(n + 2); \sqrt{x} \leq n \leq x\right\}$, $z := \sqrt{x}$ und sei $\mathcal{P}$ die Menge aller Primzahlen. Die gesiebte Menge besteht dann mindestens aus den Zahlen $p(p+2)$, für die p und $p+2$ prim ist, und daher ist $\pi_2(x) \leq \sqrt{x} + S(\mathcal{A}, \mathcal{P}, \sqrt{x})$, wenn $\pi_2(x) := \#\{p; p, p + 2 \text{ prim}\}$ die Primzahlzwillingszählfunktion bezeichnet. An diesen Beispielen sieht man, daß man an der Auswertung der Siebfunktion interessiert ist. Siebsätze liefern nun Abschätzungen für diese, typischerweise obere Abschätzungen. Das trifft auch für das **Selbergsche Sieb** zu, das wir jetzt behandeln.
Sei zunächst – etwas allgemeiner – A eine endliche Folge ganzer Zahlen mit $|A|$ vielen Folgengliedern, die wir streichen möchten. Wir gehen nun davon aus, daß wir die Anzahl $|A_d|$ der durch d teilbaren Folgengliedern von A für jedes quadratfreie $d \in \mathbb{N}$ relativ gut kennen, nämlich in der Form $|A_d| = g(d) \cdot |A| + r(d)$ mit einer multiplikativen Funktion g der Eigenschaft, daß $0 < g(p) < 1$ für alle $p \in \mathcal{P}$ gilt, und einem – hoffentlich kleinem – „Restterm“ $r(d)$.
Das Selbergsche Sieb gibt nun eine obere Abschätzung für $S(A, \mathcal{P}, z)$ in Abhängigkeit von g und r:

Satz 5.1. (Selberg–Sieb) *Sei A eine endliche Folge ganzer Zahlen mit $|A|$ vielen Folgengliedern, $\mathcal{P}$ eine Menge von Primzahlen, und für $z \geq 2$ sei $P(z) := \prod_{\substack{p<z \\ p\in\mathcal{P}}} p$. Sei die Siebfunktion $S(A,\mathcal{P},z)$ gegeben als die Anzahl der Folgenglieder a, für die $\forall\, p \in \mathcal{P}, p < z : p \nmid a$ gilt. Für jedes quadratfreie $d \in \mathbb{N}$ sei A_d die Teilfolge der durch d teilbaren Folgenglieder, und $|A_d|$ ihre Anzahl. Weiter sei gegeben eine multiplikative Funktion $g : \mathbb{N} \to \mathbb{R}_{>0}$ mit $0 < g(p) < 1$ für alle $p \in \mathcal{P}$. Sei $g_1 : \mathbb{N} \to \mathbb{R}_{>0}$ eine vollständig multiplikative Funktion, die mit g auf $\mathcal{P}$ übereinstimmt, d. h. mit $g_1(p) = g(p)$ für $p \in \mathcal{P}$. Weiter definieren wir den Restterm $r(d)$ durch $r(d) := |A_d| - g(d)\cdot|A|$ und die Funktion $G : \mathbb{R}_{\geq 2} \to \mathbb{R}_{>0}$ durch*

$$G(z) := \sum_{\substack{m<z \\ p|m\Rightarrow p\in\mathcal{P}}} g_1(m).$$

Dann gilt die Formel

$$S(A,\mathcal{P},z) \leq \frac{|A|}{G(z)} + \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)} \cdot \big|r(d)\big|,$$

wobei $\omega(d)$ wie üblich die Anzahl der verschiedenen Primteiler von d bezeichnet.

Beweis. Sei $z \geq 2$. Für jeden Teiler d von $P(z)$ suchen wir eine geeignete reelle Zahl $\lambda(d)$ mit $\lambda(1) = 1$ und $\lambda(d) = 0$ für alle $d \geq z$. Diese $\lambda(d)$ helfen bei der Abschätzung von $S(\mathcal{A},\mathcal{P},z)$, denn wegen $\big(\sum_{d|(a,P(z))} \lambda(d)\big)^2 \geq 0$ für alle $a \in \mathbb{N}$ und wegen $\big(\sum_{d|(a,P(z))} \lambda(d)\big)^2 = 1$ falls $(a,P(z)) = 1$, folgt:

$$\begin{aligned}
S(A,\mathcal{P},z) &= \sum_{\substack{a\in A \\ (a,P(z))=1}} 1 \leq \sum_{a\in A} \Big(\sum_{d|(a,P(z))} \lambda(d)\Big)^2 = \sum_{a\in A} \sum_{\substack{d_1|a \\ d_1|P(z)}} \sum_{\substack{d_2|a \\ d_2|P(z)}} \lambda(d_1)\lambda(d_2) \\
&= \sum_{d_1,d_2|P(z)} \lambda(d_1)\lambda(d_2) \sum_{\substack{a\in A \\ d_1|a,d_2|a}} 1 = \sum_{d_1,d_2|P(z)} \lambda(d_1)\lambda(d_2) \sum_{\substack{a\in A \\ [d_1,d_2]|a}} 1 \\
&= \sum_{d_1,d_2|P(z)} \lambda(d_1)\lambda(d_2)\cdot|A_{[d_1,d_2]}| \\
&= \sum_{d_1,d_2|P(z)} \lambda(d_1)\lambda(d_2)\big(g([d_1,d_2])|A| + r([d_1,d_2])\big) \\
&= |A|\cdot \sum_{d_1,d_2|P(z)} g\big([d_1,d_2]\big)\lambda(d_1)\lambda(d_2) + \sum_{d_1,d_2|P(z)} \lambda(d_1)\lambda(d_2) r\big([d_1,d_2]\big) \\
&= |A|\cdot \sum_{\substack{d_1,d_2<z \\ d_1,d_2|P(z)}} \frac{g(d_1)g(d_2)}{g\big((d_1,d_2)\big)}\cdot\lambda(d_1)\lambda(d_2) + \sum_{\substack{d_1,d_2<z \\ d_1,d_2|P(z)}} \lambda(d_1)\lambda(d_2) r\big([d_1,d_2]\big) \\
&=: |A|\cdot Q + R,
\end{aligned}$$

wobei benutzt wurde, daß $g\big([d_1,d_2]\big) = \frac{g(d_1)g(d_2)}{g\big((d_1,d_2)\big)}$ gilt, da g multiplikativ ist (Vergleiche auch Ü). Sei nun $\mathcal{D}$ die Menge aller (positiver) Teiler von $P(z)$, die $< z$ sind:

$$\mathcal{D} := \big\{k \mid P(z);\ 1 \le k < z\big\}.$$

Dies ist eine teilerabgeschlossene Menge (d. h. daß $k|d \in \mathcal{D} \Rightarrow k \in \mathcal{D}$) quadratfreier Zahlen. Ist nun $k \in \mathcal{D}$, folgt $0 < g(k) \le 1$, da $0 < g(p) < 1$ für alle $p \in \mathcal{P}$. Für $k \in \mathcal{D}$ definiere die Funktion $f : \mathbb{N} \to \mathbb{R}$ vermöge

$$f(k) := \sum_{d|k} \frac{\mu(d)}{g(k/d)} = \frac{1}{g(k)} \sum_{d|k} \mu(d)g(d) = \frac{1}{g(k)} \prod_{p|k} \big(1 - g(p)\big).$$

Dann ist $f(k) > 0$ und $f(k_1k_2) = f(k_1)f(k_2)$ für $k_1, k_2 \in \mathcal{D}$ mit $(k_1,k_2) = 1$. Möbius–Inversion, die auch auf teilerabgeschlossenen Mengen möglich ist (Ü), liefert dann, daß $\frac{1}{g(k)} = \sum_{d|k} f(d)$ gilt. Somit ist

$$\begin{aligned}
Q &= \sum_{d_1,d_2\in\mathcal{D}} \frac{1}{g\big((d_1,d_2)\big)}\, g(d_1)\lambda(d_1)g(d_2)\lambda(d_2) \\
&= \sum_{d_1,d_2\in\mathcal{D}} \sum_{\substack{k|d_1\\k|d_2}} f(k)g(d_1)\lambda(d_1)g(d_2)\lambda(d_2) \\
&= \sum_{k\in\mathcal{D}} f(k) \sum_{\substack{d_1,d_2\in\mathcal{D}\\k|d_1,k|d_2}} g(d_1)\lambda(d_1)g(d_2)\lambda(d_2) \\
&= \sum_{k\in\mathcal{D}} f(k) \Big(\underbrace{\sum_{\substack{d\in\mathcal{D}\\k|d}} g(d)\lambda(d)}_{=:y_k} \Big)^2 = \sum_{k\in\mathcal{D}} f(k) y_k^2,
\end{aligned}$$

also ist Q eine quadratische Form in den Variablen y_k, die selbst wiederum linear in den $\lambda(d)$ sind. Die duale Möbius–Inversion auf $\mathcal{D}$ angewandt zeigt nun (wir beweisen diese in einer Ü), daß

$$g(d)\lambda(d) = \sum_{\substack{k\in\mathcal{D}\\d|k}} \mu\Big(\frac{k}{d}\Big) y_k = \mu(d) \sum_{\substack{k\in\mathcal{D}\\d|k}} \mu(k) y_k, \qquad (\times)$$

insbesondere erhalten wir für $d = 1$, daß $\sum_{k\in\mathcal{D}} \mu(k)y_k = 1$.

Nun sei $F(z) := \sum_{k\in\mathcal{D}} \frac{1}{f(k)}$.

Wir wollen nun die y_k und damit die $\lambda(d)$ so einrichten, daß die quadratische Form $Q = \sum_{k\in\mathcal{D}} f(k)y_k^2$ dort ihr Minimum annimmt, wobei aber die lineare Nebenbedingung

$\otimes$: $\sum\limits_{k\in\mathcal{D}} \mu(k)y_k = 1$ erfüllt sein muß.
Dies lösen wir durch Anwenden des folgenden Lemmas:

Hilfslemma:
Seien $a_1, \ldots, a_n > 0$, $b_1, \ldots, b_n \in \mathbb{R}$. Das Minimum der quadratischen Form $Q(y_1, \ldots, y_k)$ $= a_1 y_1^2 + \cdots + a_n y_n^2$ unter der linearen Nebenbedingung $b_1 y_1 + \cdots + b_n y_n = 1$ ist gleich $m = \big(\sum\limits_{i=1}^{n} \frac{b_i^2}{a_i}\big)^{-1}$ und wird genau bei $y_i = \frac{mb_i}{a_i},\ i = 1, \ldots, n$, angenommen.

⌈ Die Cauchy–Schwarz–Ungleichung zeigt

$$1 = \Big(\sum_{i=1}^{n} b_i y_i\Big)^2 = \Big(\sum_{i=1}^{n} \Big(\frac{b_i}{\sqrt{a_i}}\Big) \cdot \sqrt{a_i} y_i\Big)^2 \overset{\oplus}{\leq} \Big(\sum_{i=1}^{n} \frac{b_i^2}{a_i}\Big) \cdot \Big(\sum_{i=1}^{n} a_i y_i^2\Big),$$

also

$$\sum_{i=1}^{n} a_i y_i^2 \geq \Big(\sum_{i=1}^{n} \frac{b_i^2}{a_i}\Big)^{-1} = m.$$

Weiterhin gilt Gleichheit in $\oplus$ genau dann, wenn es ein $t \in \mathbb{R}$ gibt mit $\sqrt{a_i} y_i = \frac{tb_i}{\sqrt{a_i}} \Leftrightarrow$ $y_i = \frac{tb_i}{a_i}$ für alle $i = 1, \ldots, n$. Dies zeigt

$$1 = \sum_{i=1}^{n} b_i y_i = t \sum_{i=1}^{n} \frac{b_i^2}{a_i} = \frac{t}{m}, \text{ also } t = m \text{ und } y_i = \frac{mb_i}{a_i}.$$

Ist umgekehrt $y_i = m\frac{b_i}{a_i}$, $i = 1, \ldots, n$, so ist $\sum\limits_{i=1}^{n} b_i y_i = 1$ und $Q(y_i, \ldots, y_n) = m$. ⌋

In unserer Situation ist das Minimum also

$$= \Big(\sum_{k\in\mathcal{D}} \frac{\mu(k)^2}{f(k)}\Big)^{-1} = \Big(\sum_{k\in\mathcal{D}} \frac{1}{f(k)}\Big)^{-1} = \frac{1}{F(z)}$$

und wird bei den $y_k = \frac{\mu(k)}{F(z)f(k)}$ angenommen.
Damit lassen sich durch Einsetzen dieser Werte für y_k in $(\times)$ dann auch die Werte für die $\lambda(d)$ ermitteln durch

$$\begin{aligned}\lambda(d) &= \frac{\mu(d)}{g(d)} \sum_{\substack{k\in\mathcal{D}\\ d|k}} \mu(k) y_k = \frac{\mu(d)}{g(d)} \sum_{\substack{d\ell<z\\ d\ell|P(z)}} \mu(d\ell) y_{d\ell} \\ &= \frac{\mu(d)}{g(d)} \cdot \sum_{\substack{\ell<z/d\\ d\ell|P(z)}} \mu(d\ell) \cdot \frac{\mu(d\ell)}{F(z)f(d\ell)}\end{aligned}$$

$$= \frac{\mu(d)}{f(d)g(d)F(z)} \underbrace{\sum_{\substack{\ell<z/d \\ d\ell|P(z)}} \frac{1}{f(\ell)}}_{=:F_d(z)},$$

wobei wir im letzten Schritt $\mu^2(d\ell) = 1$ wegen $(d,\ell) = 1$ für $d\ell|P(z)$ benutzt haben.
Wir zeigen nun, daß $\big|\lambda(d)\big| \le 1$ für $d|P(z)$ gilt: Denn es ist

$$\begin{aligned}
F(z) &= \sum_{k\in\mathcal{D}} \frac{1}{f(k)} = \sum_{\ell|d} \sum_{\substack{k\in\mathcal{D} \\ (k,d)=\ell \\ (\rightsquigarrow \ell m = k)}} \frac{1}{f(k)} = \sum_{\ell|d} \sum_{\substack{\ell m<z \\ \ell m|P(z) \\ (\ell m,d)=\ell}} \frac{1}{f(\ell m)} \\
&= \sum_{\ell|d} \frac{1}{f(\ell)} \sum_{\substack{m<z/\ell \\ \ell m|P(z) \\ (m,d/\ell)=1}} \frac{1}{f(m)} = \sum_{\ell|d} \frac{1}{f(\ell)} \sum_{\substack{m<z/\ell \\ m|P(z) \\ (m,d)=1}} \frac{1}{f(m)} \\
&= \sum_{\ell|d} \frac{1}{f(\ell)} \sum_{\substack{m<z/\ell \\ dm|P(z)}} \frac{1}{f(m)} \ge \sum_{\ell|d} \frac{1}{f(\ell)} \underbrace{\sum_{\substack{m<z/d \\ dm|P(z)}} \frac{1}{f(m)}}_{=F_d(z)(>0)} = F_d(z) \sum_{\ell|d} \frac{1}{f(\ell)} \\
&= \frac{F_d(z)}{f(d)} \sum_{\ell|d} f\Big(\frac{d}{\ell}\Big) = \frac{F_d(z)}{f(d)g(d)},
\end{aligned}$$

also ist $\big|\lambda(d)\big| = \frac{F_d(z)}{f(d)g(d)F(z)} \le 1$. Wir wollen damit nun $|R|$ abschätzen.
Dazu brauchen wir: Für eine quadratfreie Zahl $d \in \mathbb{N}$ gibt es genau $3^{\omega(d)}$ viele geordnete Paare $d_1, d_2 \in \mathbb{N}$ mit $[d_1,d_2] = d$, vergleiche auch (Ü).
Sind $d_1, d_2 < z$, so ist $d = [d_1,d_2] < z^2$.
Gilt nun $d_1, d_2|P(z)$, so ist $d = [d_1,d_2]$ quadratfrei und $d|P(z)$.
Damit läßt sich R abschätzen durch

$$\begin{aligned}
|R| &= \Big| \sum_{\substack{d_1,d_2<z \\ d_1,d_2|P(z)}} \lambda(d_1)\lambda(d_2) r\big([d_1,d_2]\big) \Big| \le \sum_{\substack{d_1,d_2<z \\ d_1,d_2|P(z)}} \big| r\big([d_1,d_2]\big) \big| \\
&\le \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)} \big| r(d) \big|, \text{ also ist} \\
S(|A|,\mathcal{P},z) &\le \frac{|A|}{F(z)} + \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)} \big| r(d) \big|.
\end{aligned}$$

Nun muß nur noch $F(z) \ge G(z)$ bewiesen werden. Mit der vollständig multiplikativen Funktion g_1, die mit g auf $\mathcal{P}$ übereinstimmt, erhält man

$$F(z) = \sum_{k\in\mathcal{D}} \frac{1}{f(k)} = \sum_{k\in\mathcal{D}} g(k) \prod_{p|k} \frac{1}{1-g(p)} = \sum_{k\in\mathcal{D}} g_1(k) \prod_{p|k} \frac{1}{1-g_1(p)}$$

$$\overset{\text{geom.}\Sigma}{=}_{0<g_1(p)<1} \sum_{k\in\mathcal{D}} g_1(k) \prod_{p|k} \sum_{r=0}^{\infty} g_1(p)^r \quad \overset{g_1}{\underset{\text{v.m.}}{=}} \sum_{k\in\mathcal{D}} g_1(k) \prod_{p|k} \sum_{r=0}^{\infty} g_1(p^r)$$

$$= \sum_{k\in\mathcal{D}} g_1(k) \sum_{\substack{\ell=1 \\ p|\ell\Rightarrow p|k}}^{\infty} g_1(\ell) = \sum_{k\in\mathcal{D}} \sum_{\substack{\ell=1 \\ p|\ell\Rightarrow p|k}}^{\infty} g_1(k\ell) = \sum_{k\in\mathcal{D}} \sum_{\substack{m=1 \\ k|m \\ p|\frac{m}{k}\Rightarrow p|k}}^{\infty} g_1(m)\cdot 1$$

$$= \sum_{m=1}^{\infty} g_1(m) \cdot \Big(\sum_{\substack{k\in\mathcal{D} \\ k|m \\ p|\frac{m}{k}\Rightarrow p|k}} 1 \Big) \geq \sum_{\substack{m<z \\ p|m\Rightarrow p\in\mathcal{P} \\ \text{(Einschränkung} \\ \text{an die } m\text{)}}} g_1(m) \cdot \Big(\sum_{\substack{k\in\mathcal{D} \\ k|m \\ p|\frac{m}{k}\Rightarrow p|k}} 1 \Big)$$

$$\geq \sum_{\substack{m<z \\ p|m\Rightarrow p\in\mathcal{P}}} g_1(m) = G(z).$$

Hier haben wir benutzt, daß die vorletzte Summe stets ≥ 1 ist, da $k = m^*$ die Summationsbedingungen erfüllt, wo $m^* := \prod_{p|m} p$ den quadratfreien Kern von m bezeichnet. Damit ist das Selberg–Sieb bewiesen. □

Nun werden wir einige wichtige Anwendungen des Selberg–Siebs besprechen.

0. Anwendung: Wir erwähnen ohne Beweis, daß das Selberg-Sieb im Falle des Eratosthenes-Modells lediglich die Abschätzung

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

bringt, also nichts Genaueres als wir auch schon anhand der oberen Tschebytschev-Abschätzung wissen. Kommen wir also zu den Anwendungen, in denen die Selberg-Siebmethode neue Erkenntnisse bringt.

1. Anwendung: Die Anzahl der Darstellungen von geraden $n \in \mathbb{N}$ als Summe zweier Primzahlen. Im Zusammenhang mit der binären Goldbach-Vermutung möchten wir ja zeigen, daß diese stets positiv ist. Die analytische Untersuchung dieser Darstellungsanzahl mit der Kreismethode liefert zwar eine Vermutung über eine Asymptotik (vgl. §3.6), aber der Fehlerterm kann dabei unkontrollierbar groß werden. Demgegenüber zeigt sich hier der Vorteil der Selberg-Siebmethode, mit der immerhin eine obere Schranke für die Darstellungsanzahl gezeigt werden kann, die von der richtigen Größenordnung ist.
Wir zeigen nämlich:

Satz 5.2. *Sei $n \in \mathbb{N}$ gerade und $R(n) := \#\big\{(p_1,p_2) \in \mathbb{P}^2;\ n = p_1 + p_2\big\}$ sei die Anzahl der Darstellungen von n als Summe zweier Primzahlen. Dann ist*

$$R(n) \ll \frac{n}{(\log n)^2} \cdot \overbrace{\prod_{p|n} \Big(1 + \frac{1}{p}\Big)}^{\ll \log\log n},$$

mit absoluter O*–Konstante.*

Beweis. Es ist $R(n) = \#\{p \in \mathbb{P};\ p \le n,\ n-p \in \mathbb{P}\}$.
Sei $a_k := k(n-k),\ A := (a_k)_{1\le k\le n}$, also ist $|A| = n$. Sei $\mathcal{P} := \mathbb{P}$ die Menge aller Primzahlen, und sei $2 < z \le \sqrt{n}$. Die Siebfunktion $S(A, \mathcal{P}, z)$ bezeichnet die Anzahl der Folgenglieder von A, die durch keine Primzahl $p < z$ teilbar sind. Ist $\sqrt{n} < k < n-\sqrt{n}$ und $a_k \equiv 0(p)$ für ein $p < z$, so ist k oder $n-k$ zusammengesetzt. Dies zeigt $R(n) \le 2\sqrt{n} + S(A, \mathcal{P}, z)$. Mit dem Selberg–Sieb können wir nun $S(A, \mathcal{P}, z)$ nach oben abschätzen. Sei g dazu vollständig multiplikativ, definiert über

$$g(p) = \begin{cases} 2/p, & \text{falls} \quad p \nmid n, \\ 1/p, & \text{falls} \quad p \mid n. \end{cases}$$

Damit ist $g_1 = g$. Da $2 \mid n$ ist $0 < g(p) < 1$ für alle $p \in \mathcal{P}$.
Und: $a_k = k(n-k) \equiv 0\ (p) \Leftrightarrow k \equiv 0\ (p) \vee k \equiv n\ (p)$.
Für $p \nmid n$ sind diese beiden Kongruenzen verschieden, für $p \mid n$ gleich.
Sei nun $d = p_1 \cdots p_h \cdot q_1 \cdots g_\ell$ eine quadratfreie Zahl, wobei $p_i \mid n, q_j \nmid n$.
Dann ist $g(d) = \frac{2^\ell}{d}$.
Da $a_k \equiv 0\ (d) \Leftrightarrow a_k \equiv 0\ (p)\ \forall p \mid d$, folgt aus dem CRS, daß es genau 2^ℓ paarweise verschiedene Kongruenzklassen mod d gibt, so daß gilt:

$$a_k \equiv 0\ (d) \Leftrightarrow k \text{ gehört zu einer dieser } 2^\ell \text{ Klassen.}$$

Somit ist dann

$$|A_d| = \sum_{\substack{k\le n \\ d\mid a_k}} 1 = \sum_{\substack{k\le n \\ k\equiv x_1(d)}} 1 + \cdots + \sum_{\substack{k\le n \\ k\equiv x_{2^\ell}(d)}} 1$$

[falls $x_1, \ldots, x_{2^\ell}$ die 2^ℓ besagten Restklassen mod d bezeichnen]

$$= 2^\ell \cdot \Big(\frac{n}{d} + \mathrm{O}(1)\Big) = 2^\ell \cdot \frac{n}{d} + \mathrm{O}(2^\ell)$$

[mit absoluter O–Konstante].

und mit $|A_d| - g(d)\cdot|A| =: r(d)$ folgt dann

$$\big|r(d)\big| = \big||A_d| - g(d)\cdot|A|\big| = \Big|2^\ell \cdot \frac{n}{d} + \mathrm{O}(2^\ell) - \frac{2^\ell}{d}\cdot n\Big| \ll 2^\ell \le 2^{\omega(d)}.$$

Mit dem Selberg–Sieb 5.1 folgt

$$S(A, \mathcal{P}, z) \le \frac{|A|}{G(z)} + \sum_{\substack{d<z^2 \\ d\mid P(z)}} 3^{\omega(d)}\big|r(d)\big| \text{ mit } G(z) := \sum_{m<z} g(m).$$

Wir wollen nun $G(z)$ nach unten abschätzen, damit wir dies weiter nach oben abschätzen können. Sei dazu

$$m = \prod_{i=1}^{h} p_i^{r_i} \prod_{j=1}^{\ell} q_j^{s_j},\ \text{wo } p_i \mid n,\quad q_j \nmid n.$$

$$\text{Dann ist } g(m) = \prod_{i=1}^{h} \Big(\frac{1}{p_i}\Big)^{r_i} \prod_{j=1}^{\ell} \Big(\frac{2}{q_j}\Big)^{s_j} = \frac{2^{s_1\cdots+s_\ell}}{m}.$$

Sei $d_n(m) := \#\big\{d \mid m;\ d \geq 1,\ (d,n) = 1\big\}$, dies ist eine modifizierte Teileranzahlfunktion. Dann ist

$$d_n(m) = d\Big(\prod_{j=1}^{\ell} q_j^{s_j}\Big) = \prod_{j=1}^{\ell}(s_j+1) \leq \prod_{j=1}^{\ell} 2^{s_j} = 2^{s_1+\cdots+s_\ell},$$

also ist $g(m) \geq \frac{d_n(m)}{m}$, und somit

$$G(z) = \sum_{m<z} g(m) \geq \sum_{m<z} \frac{d_n(m)}{m}.$$

Wegen

$$\prod_{p|n} \Big(1-\frac{1}{p}\Big)^{-1} = \sum_{\substack{t=1 \\ p|t \Rightarrow p|n}}^{\infty} \frac{1}{t}$$

folgt

$$\prod_{p|n} \Big(1-\frac{1}{p}\Big)^{-1} \cdot G(z) \geq \sum_{m<z} \frac{d_n(m)}{m} \sum_{\substack{t=1 \\ p|t\Rightarrow p|n}} \frac{1}{t} = \sum_{m<z} d_n(m) \sum_{\substack{t=1 \\ p|t\Rightarrow p|n}}^{\infty} \frac{1}{mt}$$

$$\overset{mt=w}{=} \sum_{m<z} d_n(m) \sum_{\substack{w=1 \\ m|w \\ p|(w/m)\Rightarrow p|n}}^{\infty} \frac{1}{w} = \sum_{w=1}^{\infty} \frac{1}{w} \sum_{\substack{m<z \\ m|w \\ p|(w/m)\Rightarrow p|n}} d_n(m) \geq \sum_{w<z} \frac{1}{w} \sum_{\substack{m|w \\ p|(w/m)\Rightarrow p|n}} d_n(m).$$

Sei $m|w$,

$$w = \prod_{i=1}^{h} p_i^{u_i} \prod_{j=1}^{\ell} q_j^{v_j},\ m = \prod_{i=1}^{h} p_i^{r_i} \prod_{j=1}^{\ell} q_j^{s_j} \text{ mit } p_i \mid n,\ q_j \nmid n.$$

Da $m|w$, ist

$$0 \leq r_i \leq u_i\ \forall i, \quad 0 \leq s_j \leq v_j\ \forall j, \quad \frac{w}{n} = \prod_{i=1}^{h} p_i^{u_i-r_i} \prod_{j=1}^{\ell} q_j^{v_j-s_j}.$$

In der letzten Summationsbedingung teilt jeder Primteiler von $\frac{w}{m}$ auch n, also teilt kein q_j die Zahl $\frac{w}{m}$, also ist $s_j = v_j\ \forall j$. Somit ist

$$m = \prod_{i=1}^{k} p_i^{r_i} \prod_{j=1}^{\ell} q_j^{v_j},\ \text{also } d_n(m) = \prod_{j=1}^{\ell}(v_j+1).$$

Für jedes $w \in \mathbb{N}$ ist die Anzahl solcher Teiler m gleich $\prod_{i=1}^{h}(u_i+1)$. Für jedes $w < z$ folgt somit, daß

$$\sum_{\substack{m|w \\ p|\frac{m}{w} \Rightarrow p|n}} d_n(m) = \sum_{\substack{m|w \\ p|\frac{m}{w} \Rightarrow p|n}} \prod_{j=1}^{\ell}(v_j+1) = \prod_{i=1}^{h}(u_i+1)\prod_{j=1}^{\ell}(v_j+1) = d(w).$$

Sei $z := n^{1/8}$. Dann ist

$$\prod_{p|n}\Big(1-\frac{1}{p}\Big)^{-1} G(z) \geq \sum_{w<z}\frac{d(w)}{w} \gg (\log z)^2 \gg (\log n)^2,$$

vergleiche dazu auch eine (Ü), sowie

$$\begin{aligned}\frac{|A|}{G(z)} &\ll \frac{n}{(\log n)^2}\prod_{p|n}\Big(1-\frac{1}{p}\Big)^{-1} = \frac{n}{(\log n)^2}\prod_{p|n}\Big(1-\frac{1}{p^2}\Big)^{-1}\cdot\prod_{p'|n}\Big(1+\frac{1}{p'}\Big) \\ &\ll \frac{n}{(\log n)^2}\prod_{p|n}\Big(1+\frac{1}{p}\Big), \text{ da } \prod_{p=2}^{\infty}\Big(1-\frac{1}{p^2}\Big)^{-1} \text{ konvergiert.}\end{aligned}$$

Um weiter den Fehlerterm abzuschätzen, benutzen wir $\big|r(d)\big| \ll 2^{\omega(d)}$ und erhalten

$$E := \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)}\big|r(d)\big| \ll \sum_{\substack{d<z^2 \\ d|P(z)}} 3^{\omega(d)}2^{\omega(d)} \leq \sum_{d<z^2} 6^{\omega(d)}.$$

Da $2^{\omega(d)} \leq d$, also

$$6^{\omega(d)} = \big(2^{\omega(d)}\big)^{\frac{\log 6}{\log 2}} \leq d^{\frac{\log 6}{\log 2}} < z^{2\frac{\log 6}{\log 2}},$$

folgt

$$E \leq \sum_{d<z^2} z^{2\frac{\log 6}{\log 2}} < z^{2+2\log 6/\log 2} < z^{7.2} = n^{9/10}, \text{ da } z = n^{1/8}.$$

Damit folgt

$$S(A,\mathcal{P},z) \ll \frac{n}{(\log n)^2}\prod_{p|n}\Big(1+\frac{1}{p}\Big) + n^{9/10} \ll \frac{n}{(\log n)^2}\prod_{p|n}\Big(1+\frac{1}{p}\Big),$$

und somit

$$R(n) \leq 2\sqrt{n} + S(A,\mathcal{P},z) \ll \frac{n}{(\log n)^2}\cdot\prod_{p|n}\Big(1+\frac{1}{p}\Big).$$

Die einfache Abschätzung, daß das letzte Eulerprodukt $\ll \log\log n$ ist, sei als eine (Ü)bungsaufgabe gestellt. □

2. Anwendung: Eine Abschätzung der Anzahl Primzahlzwillinge $\leq x$.
Sei $\pi_n(x) := \#\{p \in \mathbb{P};\ p \leq x \wedge p+n \in \mathbb{P}\}$ für $2 \mid n$, insbesondere ist $\pi_2(x)$ die Anzahl Primzahlzwillinge $\leq x$. Wir zeigen:

Satz 5.3. *Sei $n \in \mathbb{N}$ gerade. Dann ist* $\displaystyle \pi_n(x) \ll \frac{x}{(\log x)^2} \prod_{p \mid n} \Big(1 + \frac{1}{p}\Big),$

mit absoluter O*–Konstante.*

Beweis. Der Beweis ist ähnlich dem von Satz 5.2. Sei $\mathcal{P} := \mathbb{P}$. Sei $A = (a_k)_{1 \leq k \leq x}$ mit $a_k := k(k+n)$, also $|A| = \lfloor x \rfloor$. Für ein z mit $2 < z \leq \sqrt{x}$ sei $S(A, \mathcal{P}, z)$ wiederum die Anzahl der Elemente von A, die durch keine Primzahl $p < z$ teilbar ist. Falls $k > \sqrt{x}$ und $a_k \equiv 0\ (p)$ für ein $p < z$, ist k oder $k+n$ zusammengesetzt.
Es folgt $\pi_n(x) \leq \sqrt{x} + S(A, \mathcal{P}, z)$.
Wiederum benutzen wir das Selberg–Sieb zur Abschätzung von $S(A, \mathcal{P}, z)$. Sei $d = p_1 \cdots p_h \cdot q_1 \cdots q_\ell$ quadratfrei, wo $p_i \mid n$, $q_j \nmid n$, und $|A_d|$ die Anzahl der Folgenglieder von A, die durch d teilbar sind. Dann ist $|A_d| = \frac{|A|}{g(d)} + r(d)$, mit der gleichen Funktion g wie im Beweis von 5.2, und genauso ist $\big|r(d)\big| \ll 2^\ell \leq 2^{\omega(d)}$. Es folgt

$$S(A, \mathcal{P}, z) \leq \frac{|A|}{G(z)} + \sum_{\substack{d < z^2 \\ d \mid P(z)}} 3^{\omega(d)} \big|r(d)\big|, \text{ wo } G(z) = \sum_{m < z} \frac{1}{g(m)} \text{ ist.}$$

Der Rest des Beweises verläuft nun genau wie bei 5.2. □

Im speziellen Fall $n = 2$ halten wir fest:

Satz 5.4. *Sei $\pi_2(x)$ die Anzahl der Primzahlzwillinge $\leq x$. Dann ist* $\displaystyle \pi_2(x) \ll \frac{x}{(\log x)^2}.$

Satz 5.5. (Korollar von Satz 5.4, Satz von Brun)
Sei p_n die Folge der Primzahlzwillinge (d.h. p_n, p_n+2 prim). Dann ist $\displaystyle \sum_{n=1}^{\infty} \Big(\frac{1}{p_n} + \frac{1}{p_n+2}\Big)$
konvergent.

Beweis.

$$n = \pi_2(p_n) \overset{5.4.}{\ll} \frac{p_n}{(\log p_n)^2}, \text{ also } \frac{1}{p_n} \ll \frac{1}{n(\log n)^2},$$
$$\text{daher ist } \sum_{n=1}^{\infty} \frac{1}{p_n} \ll \sum_{n=1}^{\infty} \frac{1}{n(\log n)^2} \text{ konvergent.}$$

Die Konvergenz dieser Reihe überlegt man sich leicht mit einem Integralvergleich. □

Der Satz von Brun besagt also, daß es viel weniger Primzahlzwillinge als Primzahlen gibt. Die Frage, ob es endlich oder unendlich viele Zwillinge gibt, bleibt damit aber ungeklärt.

Die **Primzahlzwillingsvermutung** von Hardy und Littlewood aus dem Jahr 1923 besagt, daß es unendlich viele geben sollte, wieviele man genau vermutet, werden wir gleich erläutern.
Die von Brun um 1919 entwickelte Siebmethode nennt man auch das **Brunsche Sieb** und stellt eine wichtige Pionierarbeit für die moderne Siebtheorie dar. Die hier vorgestellte Siebmethode von Selberg ist eine etwas stärkere Methode, liefert für Primzahlzwillinge aber gerade den Satz 5.5 von Brun. Das noch stärkere sogenannte **große Sieb** zeigt übrigens die schärfere obere Schranke

$$\pi_2(x) \leq (16C_2 + \mathrm{o}(1))\frac{x}{\log^2 x}$$

mit der Konstanten

$$C_2 := \prod_{p\geq 3}\Big(1 - \frac{1}{(p-1)^2}\Big).$$

Man nennt diese Konstante $C_2 = 0.6601618158\ldots$ auch die **Zwillingskonstante**. Denn die berühmte Zwillingsvermutung von Hardy und Littlewood besagt, daß $\pi_2(x)$ asymptotisch wie

$$L_2(x) := 2C_2 \int_2^x \frac{du}{\log^2 u}$$

wachsen sollte. Das Ergebnis mit der Methode des großen Siebs ist also schon nahe dran, aber lediglich eine obere Schranke.
Man nennt die Konstante des Brunschen Satzes, die Zahl

$$\sum_{\substack{p,p+2\\ \text{prim}}}\Big(\frac{1}{p} + \frac{1}{p+2}\Big) = 1.9021604 \pm 5\cdot 10^{-7},$$

die **Brunsche Konstante**. Den möglichst genauen Wert dieser Konstante zu bestimmen, ist ein schwieriges numerisches Problem. Beim Versuch, diesen Wert weiter zu verbessern, fand T. Nicely um 1995 dabei einen Bug im Intel Pentium Computer Chip, genauer einen Fehler in der Fließkomma-Arithmetik des Chips. Die Behebung dieses Fehlers hat die Herstellerfirma Intel Millionen Dollar gekostet.

§ 5.2. Der Satz von Schnirelman–Goldbach

Wir zeigen in diesem § den

Satz 5.6. (Goldbach–Schnirelman)
Jede natürliche Zahl > 1 *ist die Summe einer beschränkten Anzahl von Primzahlen.*

Sei S die kleinste Zahl, so daß jedes $n \in \mathbb{N}_{>1}$ als Summe von höchstens S vielen Primzahlen geschrieben werden kann. Der Satz von Goldbach–Schnirelman besagt also, daß $S < \infty$, d. h. die Zahl S existiert.
Die Descartessche Vermutung lautet demnach $S = 3$. Den Wert für S, der sich aus dem

Beweis von 5.6. ergibt, konnte durch Verfeinerung des Beweises sukzessive von $S \leq 2 \cdot 10^{10}$ (1964) bis $S \leq 7$ (1995) verkleinert werden. Da die ternäre Goldbach–Vermutung für alle $n > 5$ unter Annahme der GRH gezeigt werden konnte (1997/98), folgt $S \leq 4$ unter Annahme der GRH.

Nun zum Beweis von Satz 5.6. Wir brauchen zunächst zwei Abschätzungen für den Mittelwert der Anzahl Darstellungen einer natürlichen Zahl als Summe zweier Primzahlen; diese werden in den nächsten zwei Lemmas bewiesen.

Lemma 5.7. *Sei $R(n)$ die Anzahl der Darstellungen von $n \in \mathbb{N}$ als Summe zweier Primzahlen. Dann ist*

$$\sum_{n \leq x} R(n) \gg \frac{x^2}{(\log x)^2}.$$

Beweis. Sind p, q prim mit $p, q \leq \frac{x}{2}$, so folgt $p + q \leq x$. Also ist

$$\sum_{n \leq x} R(n) \geq \pi\Big(\frac{x}{2}\Big)^2 \gg \frac{(x/2)^2}{(\log \frac{x}{2})^2} \gg \frac{x^2}{(\log x)^2}$$

nach dem Satz von Tschebytschev. □

Für das nächste Lemma benötigen wir die Abschätzung von Satz 5.2. für $R(n)$ nach oben, die wir in § 5.1. mit dem Selbergschen Sieb hergeleitet haben.

Lemma 5.8. *Sei $R(n)$ Die Anzahl der Darstellungen von $n \in \mathbb{N}$ als Summe zweier Primzahlen. Dann ist*

$$\sum_{n \leq x} R(n)^2 \ll \frac{x^3}{(\log x)^4}.$$

Beweis. Nach Satz 5.2 gilt für gerades n die Abschätzung

$$R(n) \ll \frac{n}{(\log n)^2} \prod_{p \mid n} \Big(1 + \frac{1}{p}\Big) \leq \frac{n}{(\log n)^2} \sum_{d \mid n} \frac{1}{d}.$$

Diese Ungleichung gilt auch für ungerade natürliche Zahlen, da eine solche Zahl nur dann als Summe zweier Primzahlen geschrieben werden kann, wenn $n - 2$ prim ist, dann ist $R(n) = 2$ und sonst $R(n) = 0$. Somit ist

$$\begin{aligned}\sum_{n \leq x} R(n)^2 &\ll \sum_{n \leq x} \frac{n^2}{(\log n)^4} \Big(\sum_{d \mid n} \frac{1}{d}\Big)^2 \ll \frac{x^2}{(\log x)^4} \sum_{n \leq x} \Big(\sum_{d \mid n} \frac{1}{d}\Big)^2 \\ &\ll \frac{x^2}{(\log x)^4} \sum_{n \leq x} \sum_{d_1 \mid n} \sum_{d_2 \mid n} \frac{1}{d_1 d_2} \leq \frac{x^2}{(\log x)^4} \sum_{d_1, d_2 \leq x} \frac{1}{d_1 d_2} \sum_{\substack{n \leq x \\ d_1 \mid n, d_2 \mid n \Leftrightarrow [d_1, d_2] \mid n}} 1\end{aligned}$$

$$\leq \frac{x^2}{(\log x)^4} \sum_{d_1,d_2\leq x} \frac{1}{d_1 d_2}\cdot\frac{x}{[d_1,d_2]} \leq \frac{x^3}{(\log x)^4}\sum_{d_1,d_2\leq x}\frac{1}{d_1^{3/2}d_2^{3/2}}$$
$$\leq \frac{x^3}{(\log x)^4}\underbrace{\Big(\sum_{d\leq x}\frac{1}{d^{3/2}}\Big)}_{kgt.} \ll \frac{x^3}{(\log x)^4},\ \text{da } [d_1,d_2]=\frac{d_1d_2}{(d_1,d_2)}\geq (d_1d_2)^{1/2}.$$

□

Mit Hilfe eines Cauchy–Schwarz–Tricks (der gleiche, den wir schon im Beweis von Satz 4.9 hatten) läßt sich mit den beiden Lemmas nun der folgende Satz zeigen:

Satz 5.9. *Die Menge $A := \{0,1\} \cup \{p+q;\ p,q \text{ prim}\}$ hat positive Schnirelmandichte.*

Beweis. Für $R(n)$ erhalten wir mit der Cauchy–Schwarz–Ungleichung, daß

$$\Big(\sum_{n\leq x} R(n)\Big)^2 \leq \sum_{\substack{n\leq x\\ R(n)\geq 1}} 1 \sum_{n\leq x} R(n)^2 \leq \underbrace{A(x)}_{\text{Zählfunktion von } A}\ \sum_{n\leq x} R(n)^2,$$

aus Lemma 5.7 und 5.8 folgt damit, daß

$$\frac{A(x)}{x} \geq \frac{1}{x}\cdot\frac{\Big(\sum\limits_{n\leq x} R(n)\Big)^2}{\sum\limits_{n\leq x} R(n)^2} \gg \frac{1}{x}\cdot\frac{x^4/(\log x)^4}{x^3/(\log x)^4} \gg 1.$$

Somit existiert $c_1 > 0$ mit $A(x) \geq c_1 x$ für alle $x \geq x_0$. Da $1 \in A$, existiert $c_2 > 0$ mit $A(x) \geq c_2 x$ für $1 \leq x \leq x_0$. Also ist $A(x) \geq \min(c_1, c_2)x$ für alle $x \geq 1$, d. h. die Schnirelmandichte ist positiv. □

Nun zum

Beweis. (von Satz 5.6., Goldbach–Schnirelman).
Die Menge $A := \{0,1\} \cup \{p+q;\ p,q \text{ prim}\}$ hat also positive Schnirelmann–Dichte.
Nach Satz 4.6 (von Schnirelman) ist A eine Basis, d. h. $\exists h : hA = \mathbb{N}_0$. Sei nun $n \geq 2$, d. h. $n-2 \geq 0$. Für $\ell, k \geq 0$ mit $\ell + k \leq h$ gibt es dann ℓ Primzahlpaare p_i, q_i mit

$$n-2 = \underbrace{1+\cdots+1}_{k \text{ Summanden}} + (p_1+q_1)+\cdots+(p_\ell+q_\ell).$$

Sei $k = 2m + r$ mit $r \in \{0,1\}$.
Falls $r = 0$, ist $n = \underbrace{2+\cdots+2}_{m+1 \text{ Summanden}} + (p_1+q_1)+\cdots+(p_\ell+q_\ell)$,
falls $r = 1$, ist $n = 3 + \underbrace{2+\cdots+2}_{m \text{ Summanden}} + (p_1+q_1)+\cdots+(p_\ell+q_\ell)$, in beiden Fällen ist also n eine Summe von höchstens $2\ell + m + 1 \leq 3h$ vielen Primzahlen. □

§ 6 Das Waring-Goldbach-Problem, Varianten und neue Wege

§ 6.1. Zum Waring-Goldbach-Problem

Wir knüpfen zunächst direkt an §5 an. Das dort besprochene Selberg-Sieb hat noch viele weitere Anwendungen. Eine weitere ist etwa der folgende Satz.

Satz 6.1. (von Romanov, 1934) *Sei $a \in \mathbb{Z}$, $a \geq 2$,*

$$A := \{p + a^k;\ p \text{ prim}, k \geq 1\},$$

$A(x)$ die Zählfunktion von A. Dann

$$\exists\, c > 0\ \forall\, x \geq x_0 : A(x) \geq cx.$$

Ein positiver Anteil aller natürlicher Zahlen kann also in der Form $p + a^k$ geschrieben werden. Weitere solche Anwendungen sind möglich.

Die Stärke der Selberg-Methode wurde bereits im vorigen §5 demonstriert: Hier konnte eine scharfe obere Abschätzung für die Darstellungsanzahl von geraden Zahlen als Summe zweier Primzahlen gegeben werden, wohingegen die analytische Kreismethode aus §3 dabei versagt hatte, wie wir dort gesehen haben.
Die Weiterentwicklung von Siebmethoden brachte daher auch neue Fortschritte.

So ist auch die beste bekannte Annäherung an die Goldbach-Vermutung ein Ergebnis weiterführender Siebtheorie. Dabei handelt es sich um den folgenden berühmten Satz von Chen. Diesen kündigte Chen schon 1966 an, doch wegen Schwierigkeiten aufgrund der chinesischen Kulturrevolution veröffentlichte er seinen Satz erst 1973.

Satz 6.2. (von Chen, 1966/1973) *Sei $n \in \mathbb{N}$, $2 \mid n$,*

$$r(n) := \#\{(p, P_2);\ n = p + P_2,\ p \text{ prim}, \Omega(P_2) \leq 2\}.$$

Dann $\exists\, n_0\ \forall\ n \geq n_0$:

$$r(n) > 0.67 \cdot \prod_{p>2} \Big(1 - \frac{1}{(p-1)^2}\Big) \prod_{\substack{p>2 \\ p \mid n}} \frac{p-1}{p-2} \cdot \frac{n}{(\log n)^2}.$$

Alle hinreichend großen geraden Zahlen lassen also eine Darstellung der Form $p + P_2$ mit einer Primzahl p und einer Fastprimzahl P_2 zu, die höchstens zwei Primfaktoren besitzt. Die Siebmethode, die Chen zum Beweis entwickelt hatte, heißt lineares Sieb. Eine Erläuterung der grundsätzlichen Ideen dieses Siebes wäre an dieser Stelle zu umfangreich, um eine vernünftige Einführung zu vermitteln. Für den Interessierten sei daher auf das Buch von Nathanson (s. Literaturhinweise) verwiesen.

Ergebnisse über Fastprimzahlen sind typisch für Anwendungen von Siebmethoden. Allgemein heißt eine natürliche Zahl n eine Fastprimzahl der Ordnung k bzw. eine Zahl vom Typ k, falls $\Omega(n) \leq k$ ist, also falls n insgesamt höchstens k Primfaktoren besitzt. Für eine Fastprimzahl der Ordnung k hat sich auch die kurze Schreibweise P_k eingebürgert.

Eine weitere Annäherung an das Goldbach-Problem ist bekannt als das Goldbach-Waring-Problem. Für eine eingehendere Erläuterung dieses Problems gehen wir nochmal kurz zum Waring-Problem zurück, das wir in §4 mit der Linnik-Methode gelöst hatten.

Dort haben wir gezeigt, daß es für jedes $k \in \mathbb{N}_{\geq 2}$ eine Zahl $g(k)$ gibt, so daß jedes $n \in \mathbb{N}$ als Summe von höchstens $g(k)$ vielen k-ten Potenzen, also als

$$n = x_1^k + \cdots + x_l^k,\ l \leq g(k),\ x_1, \ldots, x_l \in \mathbb{N},$$

geschrieben werden kann. Fordert man dies nur für alle hinreichend großen n, ist die dafür nötige Summandenanzahl $G(k)$ höchstens so groß wie $g(k)$.

Nun liefert die Kreismethode, die wir in §3 am Beispiel des ternären Goldbach-Problems kennengelernt haben, Ergebnisse für die Darstellungsanzahl

$$R_{k,s}(n) := \#\{(x_1, \ldots, x_s) \in \mathbb{Z}_{>0}^s;\ n = x_1^k + \cdots + x_s^k\}$$

im Waring-Problem. Hardy und Littlewood zeigten dafür folgenden Satz.

Satz 6.3. (Hardy und Littlewood, 1919/1920) *Sei $k \geq 2$. Ist $s \geq 2^k + 1$, dann ist*

$$R_{k,s}(n) \sim \frac{\Gamma^s(1+\frac{1}{k})}{\Gamma(\frac{s}{k})} \mathcal{S}_{k,s}(n) \cdot n^{\frac{s}{k}-1} \qquad (*)$$

für $n \to \infty$, wobei Γ die (Eulersche) Γ-Funktion bezeichnet, und $\mathcal{S}_{k,s}(n) \geq c_1(k,s) > 0$ die singuläre Reihe des Waring-Problems.

Auf den genauen Wert der singulären Reihe gehen wir hier nicht näher ein, wichtig ist, daß sie für die angegebenen s und k stets positiv ist. Denn damit ist die Darstellungsanzahl $R_{k,s}(n)$ für große n ebenfalls positiv – was bedeutet, daß das Waringproblem für k und s und hinreichend große n lösbar ist.

Eine untere Schranke der Summandenanzahl s nach unten ist erforderlich, damit der Beweis geführt werden kann. Das ist nicht weiter verwunderlich, ist doch für $s = 2$ und $k \geq 3$ das Fermatsche Problem inbegriffen: k-te Potenzen können nicht Summe zweier k-ten Potenzen sein, wie man seit dem Beweis der Fermatschen Vermutung von A. Wiles weiß.
Daher ist interessant zu wissen, wie groß hier die kleinstmögliche Summandenanzahl s ist. Sei $\tilde{G}(k)$ das kleinste s, so daß obige Asymptotik (*) gilt. Ford zeigte 1995, daß

$$\tilde{G}(k) \leq k^2(\log k + \log\log k + \mathrm{O}(1)) \qquad (**)$$

für $k \to \infty$ gilt. Vaughan (1986) und Boklan (1994) erhielten die Schranken $\tilde{G}(k) \leq 2^k$ für $k \geq 3$ und $\tilde{G}(k) \leq \frac{7}{8} \cdot 2^k$ für $k \geq 6$, was für $k \leq 8$ besser ist als die Schranke in (**).

Nun zum Waring-Goldbach-Problem. Hier fragt man nach Lösungen der Gleichung

$$n = p_1^k + \cdots + p_s^k,$$

also welche $n \in \mathbb{N}$ sich als Summe von s vielen k-ten Primzahlpotenzen geschrieben werden können. Dies ist natürlich schärfer als das Waring-Problem, und für $s = 2$ und $k = 1$ ist diese Frage gerade das offene binäre Goldbachproblem.
In welchen Fällen das Waring-Goldbach-Problem gelöst werden kann, besagt nun der folgende Satz von Vinogradov (1937) und Hua (1938).

Satz 6.4. (Vinogradov und Hua, aktuelle Version) *Seien $k, s, n \in \mathbb{N}$, und*

$$R_{k,s}^*(n) := \#\{(p_1, \ldots, p_s);\ n = p_1^k + \cdots + p_s^k,\ p_i \in \mathbb{P}\}.$$

Sei

$$s \geq \begin{cases} 2^k + 1, & 1 \leq k \leq 5, \\ \frac{7}{8} \cdot 2^k + 1, & 6 \leq k \leq 8, \\ k^2(\log k + \log\log k + \mathrm{O}(1)), & k > 8. \end{cases}$$

Dann ist

$$R_{k,s}^*(n) \sim \frac{\Gamma^s(1 + \frac{1}{k})}{\Gamma(\frac{s}{k})} \mathcal{S}_{k,s}^*(n) \frac{n^{\frac{s}{k}-1}}{(\log n)^s}$$

für $n \to \infty$. Die (absolut konvergente) singuläre Reihe ist

$$\mathcal{S}_{k,s}^*(n) \geq c_2(k, s) > 0,$$

falls $n \equiv s \bmod K(k)$, wobei

$$K(k) := \prod_{(p-1)|k} p^{\gamma(k,p)}, \qquad \gamma(k,p) := \begin{cases} \theta + 2, & p = 2,\ 2 \mid k, \\ \theta + 1, & \textit{sonst,} \end{cases} \qquad \textit{mit } p^\theta || k.$$

Die Kongruenzbedingung $\equiv s \bmod K(k)$ ist nötig, damit die singuläre Reihe positiv ist. Das sieht man z. B. auch im Spezialfall des ternären Goldbachproblems für $k = 1$ und $s = 3$, bei dem $K(k) = 2$ ist; hier betrifft die Kongruenzbedingung genau alle ungeraden n. Der Satz von Vinogradov aus §3 ist also Teil dieses sehr allgemeinen Satzes von Vinogradov und Hua zum Waring-Goldbach-Problem.
Wir ziehen noch weitere Folgerungen aus diesem Satz für Primzahlquadrate ($k = 2$) und Primzahlkuben ($k = 3$):

Satz 6.5. (Korollar) *Jedes hinreichend große $n \equiv 5$ (24) ist Summe von 5 Primzahlquadraten.*

(Denn für $k = 2$, $s = 5$ ist $K(k) = 2^3 \cdot 3^1 = 24$.)

Satz 6.6. (Korollar) *Jede hinreichend große ungerade Zahl ist Summe von* 9 *Primzahlkuben.*

(Denn für $k = 3$, $s = 9$ ist $K(k) = 2$.)

Wiederum von Interesse ist die kleinste Summandenanzahl s, für die das Waring-Goldbach-Problem lösbar ist. Sei dazu

$$H(k) := \min\{s;\ n = p_1^k + \cdots + p_s^k \text{ lösbar für alle hinreichend großen } n \equiv s\ (K(k))\}.$$

Man vermutet, daß $H(k) = k + 1$ ist, allerdings konnte dies bisher für kein k bewiesen werden. Für $k = 1$ bedeutet $H(1) = 2$ ja gerade die Gültigkeit der binären Goldbach-Vermutung für große gerade n. Die besten bekannten Schranken für $k \leq 3$ sind durch den Satz von Hua und Vinogradov gegeben, also $H(1) \leq 3$ (ternäres Goldbach-Problem), $H(2) \leq 5$, $H(3) \leq 9$.

Für $k \geq 4$ fassen wir die bestbekannten Ergebnisse zu folgendem Satz zusammen:

Satz 6.7. *Sei $k \geq 4$, $H(k)$ wie oben. Dann ist*

$$H(k) \leq \begin{cases} F(k), & 4 \leq k \leq 10, \\ k(4\log k + 2\log\log k + \mathrm{O}(1)), & k > 10, \ \text{(Hua)} \end{cases}$$

wobei $F(k)$ wie folgt gegeben ist:

k	4	5	6	7	8	9	10
$F(k)$	14	21	33	46	63	83	107

Die Schranke $k(4\log k + 2\log\log k + \mathrm{O}(1))$ kann für hinreichend große k noch verbessert werden zu

$$H(k) \leq k\Big(\frac{3}{2}\log k + \mathrm{O}(\log\log k)\Big), \text{ für } k \to \infty.$$

(Hua/Wooley 1995)

§ 6.2. Weitere additive Probleme mit Primzahlen

Es gibt noch viele weitere Möglichkeiten, Varianten und Verallgemeinerungen des Waring-Goldbach-Problems zu formulieren, z. B. kann man die diophantische Gleichung

$$n = a_1 p_1^k + a_2 p_2^k + \cdots + a_s p_s^k$$

betrachten, wo $n, a_1, \ldots, a_s$ feste ganze Zahlen sind, nicht notwendig positiv.
Wenn die Gleichung lösbar ist, möchte man auch die Lösungen mit $p_1, \ldots, p_s \leq X$ zählen, wenn X ein großer Parameter ist.

Zum Beispiel ist schon die Zwillingsvermutung $p_1 - p_2 = 2$ von diesem Typ. (Also die Frage, ob $p_1 - p_2 = 2$ unendlich viele Lösungen hat.) Diese ist eng mit dem binären Goldbachproblem verwandt, wie wir auch schon im §5 bei der Behandlung des Selberg-Siebs gesehen haben. Nun läßt sich auch der Beweis des Satzes von Chen so umformulieren, daß sich folgende Annäherung an die Zwillingsvermutung ergibt:

Satz 6.8. (Chen) *Es gibt unendlich viele Primzahlen p mit $p + 2 = P_2$.*

Das bedeutet, daß die Gleichung $p + 2 = p'$ oder die Gleichung $p + 2 = p_1 p_2$ unendlich viele Lösungen hat – vermutlich haben dies beide.
Aber auch schon die schwächere Vermutung, ob $\Omega(p + 2)$ gerade (respektive ungerade) für unendlich viele Primzahlen p ist, ist völlig offen.
Aufgrund der strukturellen Ähnlichkeit des Zwillingsproblems mit dem Goldbach-Problem lassen sich etliche Goldbach-Ergebnisse auf die Zwillingsvermutung übertragen, so auch der folgende Satz:

Satz 6.9. (Pintz 2007) *Für $E'(x) := \#\{n \leq x, 2 \mid n, n \neq p_1 - p_2\}$ gilt $E'(x) \ll x^{2/3}$.*

Fast alle geraden n sind daher Differenz zweier Primzahlen; oder anders ausgedrückt: Fast alle geraden n sind Abstand zwischen zwei Primzahlen. Ob diese dann auch unendlich viele Darstellungen als Differenz zweier Primzahlen haben, ist unbekannt.

Andere Varianten des Waring-Goldbach-Problems betrachten diophantische Gleichungen des Typs

$$n = f(p_1) + f(p_2) + \cdots + f(p_s)$$

mit einem Polynom $f(X) \in \mathbb{Z}[X]$.

Auch Systeme von solchen Gleichungen werden behandelt, z. B.

$$n_j = p_1^j + p_2^j + \cdots + p_s^j, \quad 1 \leq j \leq k.$$

Die Lösungsanzahl erfüllt ebenso eine asymptotische Formel wie in dem Satz von Vinogradov und Hua, wobei der Hauptterm dabei aber weniger gut verstanden ist.

Ein sehr klassisches Problem, bei dem natürlicherweise ein System von diophantischen Gleichungen auftaucht, ist die Frage nach der Existenz (nichttrivialer) arithmetischer Progressionen (APs) bestehend aus r Primzahlen. Genauer ausgedrückt: Gibt es für jedes $r \geq 3$ unendlich viele Paare p, k einer Primzahl p und einer natürlichen Zahl k, so daß die Zahlen $p, p + k, p + 2k, \ldots, p + (r - 1)k$ allesamt Primzahlen sind? (Für $r = 2$ ist die Aussage trivial.)
Noch anders ausgedrückt: Wir suchen Lösungen des diophantischen Systems

$$p_i - 2p_{i+1} + p_{i+2} = 0, \quad 1 \leq i \leq r - 2,$$

d. h. der Abstand zwischen zwei Primzahlen p_i, p_{i+1}, $1 \leq i \leq r - 1$, der Folge ist immer gleich. Das Problem lautet, ob dieses System unendlich viele Lösungen mit paarweise verschiedenen Primzahlen besitzt.

Für $r = 3$ kann dies mit einer Variante des in §3 vorgestellten Vinogradov-Beweises des ternären Goldbach-Problems gezeigt werden, für $r > 3$ liegt das Problem jedoch außerhalb der Reichweite der Kreismethode.

Weitere Teilergebnisse in diese Richtung waren bislang folgende Sätze:

Heath-Brown 1981: Es gibt unendlich viele APs aus 3 Primzahlen und einer P_2-Fastprimzahl.

Balog 1992: Für alle r gibt es paarweise verschiedene Primzahlen $p_1, \ldots, p_r$, so daß alle Mittelwerte $(p_i + p_j)/2$ prim sind.

2004 wurde die Vermutung über Primzahlen in arithmetischen Progressionen jedoch in voller Allgemeinheit bewiesen. T. Tao und B. Green zeigten den folgenden Satz:

Satz 6.10. (Tao/Green 2004) *Sei $k \geq 3$, $\mathcal{A} \subseteq \mathbb{P}$,*

$$\limsup_{N \to \infty} \frac{\#\{n \in \mathcal{A}; n \leq N\}}{\pi(N)} > 0.$$

Dann enthält $\mathcal{A}$ unendlich viele APs aus k Elementen.

Insbesondere ist die Voraussetzung des Satzes für $\mathcal{A} = \mathbb{P}$ erfüllt, woraus die Gültigkeit der Vermutung über Primzahlen in Progressionen folgt. Jedoch ist der Beweis des Satzes von Tao und Green ein reiner Existenz-Beweis, für die Konstruktion beliebig langer Primzahl-Progressionen gibt er keinen Hinweis. Dennoch handelt es sich um ein sehr bemerkenswertes Ergebnis, bei dem Tao und Green neue Wege der additiven Kombinatorik erschlossen haben.

§ 6.3. Weitere Arbeiten zum Waring-Goldbach-Problem

§ Abschätzungen von Ausnahmemengen

Wie die Ausnahmen im binären Goldbach-Problem kann man auch die Ausnahmen des Waring-Goldbach-Problems behandeln und Abschätzungen für ihre Anzahl zeigen.
Sei k, s gegeben und sei

$$E_{k,s}(x) := \#\{n \leq x;\ n \equiv s\ (K(k)),\ n = p_1^k + \cdots + p_s^k \text{ unlösbar in } p_1, \ldots, p_s \in \mathbb{P}\}$$

die Anzahl der Ausnahmen im Waring-Goldbach-Problem. ($K(k)$ ist der im Satz von Vinogradov und Hua definierte Modul.)
Erste nichttriviale Abschätzungen für diese Ausnahmen konnte Hua angeben, weitere folgten, z. B. Schwarz 1961: $\forall A > 0$: $E_{k,s}(x) \ll \frac{x}{(\log x)^A}$ für gewisse k, s.
Weitere Ergebnisse für spezielle k und s sind (von diversen Autoren):
$E_{2,3}(x) \ll x^{6/7+\varepsilon}$, $E_{2,4}(x) \ll x^{5/14+\varepsilon}$, $E_{3,s}(x) \ll x^{1-\frac{s-4}{153}}$ ($5 \leq s \leq 8$, was noch verbessert wurde), $E_{k,s}(x) \ll x^{1-\delta}$ für $\delta = \delta(k,s) > 0$ explizit für alle $k \geq 4$ und s, für die auch $E_{k,s}(x) \ll \frac{x}{(\log x)^A}$ gilt.

§ Das Waring-Goldbach-Problem mit Fast-Primzahlen

Betrachtet man z. B. die Lagrange-Gleichung

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2,$$

so konnte gezeigt werden, daß jedes hinreichend große $n \not\equiv 0, 1, 5$ (8) in dieser Art mit x_1, x_2 prim und $x_3, x_4 \in \mathbb{Z}$ geschrieben werden kann. [Greaves] Die zugehörige Asymptotik ist hier bekannt.
Weitere Ergebnisse hierzu: Jedes hinreichend große $n \equiv 4$ (24) kann als Summe von vier Quadraten aus P_{25}-Zahlen geschrieben werden. [Brüdern/Fouvry bzw. Heath-Brown/Tolev]
Dies geht auch mit x_1 prim und x_2, x_3, x_4 vom Typ P_{101}. [Heath-Brown/Tolev]
Und: Ist $n \equiv 3$ (24), $5 \nmid n$ hinreichend groß, so ist n Summe dreier Fast-Primzahlen vom Typ P_{521}. Ist n zusätzlich quadratfrei, so sind können diese vom Typ P_{371} gewählt werden. [Blomer/Brüdern]
Man weiß aber auch, daß fast alle $n \leq x$ (bis auf $\mathrm{O}((\log x)^{6+\varepsilon})$ viele) als $n = x_1^2 + \cdots + x_4^2$ mit x_1, x_2, x_3 prim und $x_4 \in \mathbb{Z}$ darstellbar sind. [Wooley]

Für Kuben kennt man folgende Ergebnisse:
Ist n groß, so ist $n = x^3 + p_1^3 + \cdots + p_7^3$ lösbar mit Primzahlen p_i und $x \in \mathbb{Z}$. Für $n \equiv 4$ (18) kann x dabei als eine P_4-Zahl gewählt werden. [Roth 1951 bzw. Brüdern]
Ist n groß, so ist $n = p_1^3 + x_1^3 + \cdots + x_6^3$ mit p_1 prim und $x_i \in \mathbb{Z}$ mit $x_1, \ldots, x_5$ vom Typ P_5 und x_6 vom Typ P_{69}. [Brüdern]
Ist n groß, so ist $n = x_1^3 + \cdots + x_7^3$ mit $x_i \in \mathbb{Z}$ vom Typ P_4. [Kawada]

§ Das Waring-Goldbach-Problem mit eingeschränkten Variablen

Das ternäre Goldbachproblem kann man auch verschärfen, indem man zusätzliche Bedingungen an die drei Primzahlen stellt, deren Summe eine ungerade Zahl n ergeben. Z. B. die Bedingung, daß alle drei Primzahlen etwa von der gleichen Größe, also etwa $n/3$ sind. Der Beweis von Vinogradov läßt sich dahingehend abwandeln, und so wurde gezeigt, daß gilt:
Ist n hinreichend groß und ungerade, so ist $n = p_1 + p_2 + p_3$ mit drei Primzahlen, für die jeweils

$$\left| p_i - \frac{n}{3} \right| \leq n^{63/64+\varepsilon}$$

gelten [Haselgrove 1951]. Diese Abschätzung konnte inzwischen zu $n^{4/7}$ verbessert werden [Baker/Harman].
Für die Darstellung von n als Summe von 5 Primzahlquadraten etwa gleicher Größe gilt ein analoges Ergebnis:
Ist $n \equiv 5$ (24) groß, so ist $n = p_1^2 + \cdots + p_5^2$ mit p_i prim und

$$\left| p_i^2 - \frac{n}{5} \right| < n^{45/46+\varepsilon},$$

und unter Annahme der GRH läßt sich dies zu $n^{19/20+\varepsilon}$ verbessern [Liu/Zhan].
1986 zeigte E. Wirsing die Existenz dünner Primzahlmengen $\mathcal{S}$, so daß jedes hinreichend große ungerade n als Summe dreier Primzahlen von $\mathcal{S}$ geschrieben werden kann. Der Beweis ist probabilistisch, d. h. leider nicht konstruktiv.
Das erste konstruktive Beispiel dazu sind die Piatetski-Shapiro-Primzahlen

$$\mathcal{P}_c = \{p;\ p = \lfloor n^c \rfloor \text{ für ein } n \in \mathbb{N}\}.$$

Für $1 < c < 16/15$ liefern diese eine dünne Menge von Primzahlen, die im ternären Goldbach-Problem als Summanden dienen können. [Balog/Friedlander, Jia]
Eine weitere Möglichkeit, die Primzahlen im ternären Goldbachproblem einzuschränken, ist zu fordern, daß die $p_i + 2$ Fast-Primzahlen sind.
Hier weiß man: Ist $n \equiv 3\ (6)$ groß, so ist $n = p_1 + p_2 + p_3$, mit $p_1 + 2 = P_2$, $p_2 + 2 = P_5$, $p_3 + 2 = P_7$. [Tolev]
Dazu ist auch die Behauptung von Tao und Green interessant, daß es wohl unendlich lange nichttriviale APs aus Primzahlen p gibt, für die $p + 2 = P_2$ ist. Für Progressionen aus 3 Primzahlen haben Tao und Green ihre Behauptung bereits veröffentlicht.

§ Additive Probleme mit gemischten Potenzen

Die Hardy-Littlewoodsche Kreismethode liefert eine asymptotische Formel für die Anzahl der Darstellungen der Lösungen von

$$n = p + x^2 + y^2, \qquad p \text{ prim}, x, y \in \mathbb{Z}.$$

[Hardy/Littlewood, Hooley, Linnik]
Weiter vermuteten Hardy und Littlewood eine asymptotische Formel für die Anzahl der Darstellungen von n als $n = p + x^2$, welche bis heute unbewiesen ist. Man weiß jedoch, daß diese Vermutung für fast alle $n \le x$ gilt:
Ist für $k \ge 2$

$$E_k(x) := \#\{n \le x;\ n = p + x^k \text{ unlösbar}\}$$

die Anzahl der Ausnahmen, so gilt

$$E_2(x) \ll \frac{x}{(\log x)^A}.$$

[Miech]
Weitere Verbesserungen folgten, so etwa, daß $E_k(x) \ll x^{1-\delta_k}$ mit einer Konstanten $\delta_k > 0$ ist. Nimmt man die GRH an, so gilt $E_k(x) \ll x^{1-\delta_k}$ mit $\delta_k = \frac{1}{k \cdot 2^k}$ für $2 \le k \le 4$ bzw. $\delta_k = \frac{1}{25k}$ für $k \ge 5$. [diverse Autoren]
Und ein Ergebnis mit gemischten Potenzen lautet: Ist $3 \le k \le 5$, so ist für alle großen n die Gleichung $n = x + p_1^2 + p_2^3 + p_3^k$ lösbar, wo die p_i prim sind und x eine P_2-Fastprimzahl. [Brüdern/Kawada]

§ **Waring-Goldbach-Problem „mit Koeffizienten“**

Die Gleichung

$$n = a_1 p_1^k + a_2 p_2^k \cdots + a_s p_s^k$$

kann in zwei verschiedenen Kontexten behandelt werden:
(I) Angenommen, alle a_i und n sind von gleichem Vorzeichen.
Dann erwartet man Lösungen für große $|n|$ (d. h. wenn $|n| \geq C(a_1, \ldots, a_s)$ ist). Ist $|n|$ nicht zu groß im Vergleich zu $|a|_\infty := \max\{|a_1|, \ldots, |a_s|\}$, ist das Problem schwieriger.
(II) Angenommen, die a_i sind nicht alle von gleichem Vorzeichen. Dann sucht man Lösungen in Primzahlen p_i, die nicht zu groß im Vergleich zu $|a|_\infty$ und $|n|$ sind.
Teilergebnisse dazu sind die folgenden:
Es gibt Lösungen, falls

- $k = 1$, $s = 3$: a_1, a_2, a_3 mit gleichem Vorzeichen und $|n| \gg |a|_\infty^A$ für $A > 0$.
- $k = 1$, $s = 3$: a_1, a_2, a_3 mit verschiedenen Vorzeichen und mit $\max_{p_1,p_2,p_3} \ll |a|_\infty^{A-1} + |n|$.

Dabei müssen die a_i bestimmten Kongruenzbedingungen genügen. [Liu/Tsang]
Bekannt ist, daß $A = 38$ dies erfüllt, was unter weiteren Voraussetzungen noch verkleinert werden kann.
Auch im Fall $s = 5$ und $k = 2$ gibt es Lösungen, falls

- $a_1, \ldots, a_5$ vom gleichen Vorzeichen und $|n| \gg |a|_\infty^{15+\varepsilon}$
- $a_1, \ldots, a_5$ von verschiedenen Vorzeichen und $\max\{p_1, \ldots, p_5\} \ll |a|_\infty^{7+\varepsilon} + |n|^{1/2}$.

[diverse Autoren]

§ **Das Goldbach-Linnik-Problem**

Linnik zeigte 1951/1953 folgende Annäherung an die Goldbachsche Vermutung:

Satz 6.11. (Linnik) *Alle geraden $n \geq 2$ sind darstellbar in der Form*

$$n = p_1 + p_2 + 2^{a_1} + \cdots + 2^{a_K}$$

mit K vielen 2er-Potenzen.

Klar ist, daß die Behauptung $K = 0$ in diesem Satz äquivalent zur Gültigkeit der binären Vermutung ist.
Die Konstante K wurde sukzessive verbessert, inzwischen weiß man, daß $K = 13$ und $K = 7$ unter Annahme der GRH gilt [Heath-Brown, Puchta 2002], bzw. $K = 8$ und $K = 7$ unter Annahme der GRH [Ruzsa, Pintz 2003].

§ 6.4. Große und kleine Lücken zwischen aufeinanderfolgenden Primzahlen

Hier handelt es sich eher weniger um ein additives Problem, paßt aber noch ganz gut als Abschluß zu unserem kleinen Streifzug in die Primzahltheorie, auch, weil sich hier interessante Neuerungen in jüngster Zeit ergeben haben, die wir nicht unerwähnt lassen wollen.

Sei $d_n := p_{n+1} - p_n$ die Differenz zwischen zwei aufeinanderfolgenden Primzahlen p_n und p_{n+1}, also der Abstand der Primzahllücke zwischen p_n und p_{n+1}.
Wenn wir obere Abschätzungen für diese Lücken angeben, so zeigen wir, daß es keine größeren Lücken zwischen Primzahlen geben kann. Also schätzen wir insbesondere große Lücken ab.

Schon früh kannte man die Abschätzung $d_n \ll p_n^{\vartheta_1}$ mit einer Konstanten $\vartheta_1 > 0$.
Hoheisel konnte 1930 den Wert $\vartheta = 1 - \frac{1}{33000}$ bestimmen.
Daraufhin folgten mehrere Verbesserungen, etwa die von Ingham 1973, der $\vartheta_1 = 5/8 + \varepsilon$ zeigen konnte. Dieses Ergebnis lieferte dann erstmals die Möglichkeit zu zeigen, daß zwischen zwei beliebigen aufeinanderfolgenden Kubikzahlen m^3 und $(m+1)^3$ stets eine Primzahl existiert. (Wir haben dies in einer (Ü) schon unter Annahme der RH gezeigt.)
Von Huxley 1972 stammt der Wert $\vartheta_1 = \frac{7}{12} + \varepsilon$.
Baker, Harman und Pintz zeigten 2001, daß $\vartheta_1 = 21/40$ ein zulässiger Wert für ϑ_1 ist.

Unter Annahme der RH kann man $d_n \ll \sqrt{n} \log n$ zeigen (Cramér 1920), doch selbst mit dieser unter der RH verbesserten Abschätzung ist es nicht möglich, daraus die Existenz einer Primzahl zwischen zwei beliebigen aufeinanderfolgenden Quadratzahlen m^2 und $(m+1)^2$ zu folgern.
Die empirische Untersuchung mit Zahlendaten zeigt hier, daß in etwa die Abschätzung $d_n < 2\sqrt{p_n}$ gelten müßte. Diese würde gerade dazu ausreichen, um die Vermutung über die Existenz von Primzahlen zwischen zwei beliebigen aufeinanderfolgenden Quadratzahlen zu zeigen.
Das Brunsche Sieb zeigt, daß immerhin eine P_{11}-Fastprimzahl in jedem Intervall $(x, x + \sqrt{x})$, x hinreichend groß, liegen muß. Mit der Methode von Chen läßt sich dies sogar für eine P_2-Fastprimzahl nachweisen.

Zu der Behandlung von Primzahllücken kommt oft das Cramérsche Wahrscheinlichkeitsmodell für Primzahlen (kurz: CM) zum Einsatz, das durch den Primzahlsatz nahegelegt wird. Bei diesem definiert man eine Folge ξ_n von Zufallsvariablen für $n \geq 3$ mit $P(\xi_n = 1) = \frac{1}{\log n}$ und $P(\xi_n = 0) = 1 - \frac{1}{\log n}$. Dies modelliert also unsere Heuristik aus dem Primzahlsatz, daß eine natürliche Zahl $n \geq 3$ mit Wahrscheinlichkeit $\frac{1}{\log n}$ eine Primzahl ist.
Legt man dieses Wahrscheinlichkeitsmodell CM zugrunde, kommt man zu der Aussage,

daß $\limsup_{n\to\infty} \frac{d_n}{(\log p_n)^2} = 1$ mit Wahrscheinlichkeit 1 in CM gilt. Und auch, daß $\pi(x+y) - \pi(x) \sim \frac{y}{\log x}$ für $y = (\log x)^\lambda$, $\lambda > 2$, gelten müßte.

Beide Vermutungen konnten inzwischen widerlegt werden. Somit wurde die Einsicht gewonnen, daß das Cramérsche Modell seine Grenzen hat; wir haben es eben mit Primzahlen und nicht mit echten unabhängigen Zufallsvariablen zu tun.

Es ist jedoch möglich, das Cramérsche Modell so zu korrigieren (kurz CCM für „corrected Cramér's model"), daß man damit die wohl korrekte Vermutung für die Größe großer Primzahllücken aussprechen kann, nämlich

$$\limsup_{n\to\infty} \frac{d_n}{\log^2 p_n} = 2e^{-\gamma}$$

mit Wahrscheinlichkeit 1 in CCM. Die reelle Zahl γ ist hier die Eulersche Konstante.

§ Untere Schranken für große Primzahllücken/Das Erdős-Rankin-Problem

Aus dem Primzahlsatz folgt, daß

$$\lambda := \limsup_{n\to\infty} \frac{d_n}{\log n} \geq 1$$

gilt, das heißt, daß es unendlich oft größere Primzahllücken als $\log n$ gibt (wenn p_n die kleinere Primzahl ist).
1931 zeigte Westsynthius, daß $\lambda = \infty$ ist, nämlich daß

$$\limsup_{n\to\infty} \frac{d_n}{\log p_n \log_{(3)} p_n / \log_{(4)} p_n} \geq 2e^{\gamma},$$

wobei $\log_{(k)} n = \underbrace{\log\log\ldots\log}_{k \text{ mal}} n$ den k-fach-iterierten Logarithmus bezeichnet.
Erdős zeigte 1935, daß

$$\limsup_{n\to\infty} \frac{d_n}{\log p_n \log_{(2)} p_n \log_{(4)} p_n / (\log_{(3)} p_n)^2} > 0,$$

was 1938 von Rankin verbessert wurde zu

$$\limsup_{n\to\infty} \frac{d_n}{\log p_n \log_{(2)} p_n \log_{(4)} p_n / (\log_{(3)} p_n)^2} \geq c_0$$

mit dem Wert $c_0 = \frac{1}{3}$. Erdős vermutete, daß $c_0 = \infty$ ist und setzte einen Preis von 10 000 US-Dollar für einen Beweis aus, den höchsten Preis, den Erdős jemals aussetzte.
Der bislang beste bekannte Wert ist $c_0 = 2e^{\gamma}$ von Pintz aus dem Jahr 1997.

§ Kleine Primzahllücken

Sei $\Delta_1 := \liminf_{n\to\infty} \frac{d_n}{\log p_n}$, laut Primzahlsatz ist $\Delta_1 \leq 1$.
Hardy und Littlewood zeigten 1926 mit der Kreismethode, daß unter Annahme der GRH die Abschätzung $\Delta_1 \leq \frac{2}{3}$ folgt.
Rankin verbesserte dies 1940 zu $\Delta_1 \leq \frac{3}{5}$ unter Annahme der GRH, und Erdős konnte im gleichen Jahr die Existenz einer Konstante $c > 0$ zeigen mit $\Delta_1 < 1 - c$, ohne daß eine unbewiesene Vermutung zugrunde liegt.
Bald darauf wurden explizite Zahlenwerte für c gefunden, und weitere Verbesserungen für die obere Abschätzung von Δ_1 waren etwa 15/16 und 29/32. [Ricci, Wang/Xie/Yu]

Im Jahr 1966 zeigten Bombieri und Davenport, daß $\Delta_1 \leq \frac{1}{2}$ gilt, indem der Satz von Bombieri-Vinogradov anstatt der GRH eingesetzt wurde.
Die Kombination ihrer Methode mit der von Erdős zeigte dann, daß $\Delta_1 \leq \frac{2+\sqrt{3}}{8} = 0.4667\ldots$ gilt. Weitere Verbesserungen folgten, bis Maier 1988 zeigte, daß $\Delta_1 \leq 0.2484\ldots$ gilt, was bis 2005 die beste obere Abschätzung für Δ_1 blieb.

Man vermutete, daß der Wert von Δ_1 gleich 0 ist; man kennt diese Vermutung auch als die „small gap conjecture“.
Stärker ist die „bounded gap conjecture“, die besagt, daß $\liminf_{n\to\infty}(p_{n+1} - p_n) < \infty$ ist. Stimmt die Primzahlzwillingsvermutung, d. h. gibt es unendlich viele Primzahlzwillinge, so müßte dieser Wert ja $= 2$ sein sein.

2007 konnte die small gap conjecture von Goldston, Pintz und Yildirim gezeigt werden, ja sogar daß

$$\liminf_{n\to\infty} \frac{d_n}{(\log p_n)^{1/2}(\log\log p_n)^2} < \infty.$$

Unter Annahme der unbewiesenen Elliott-Halberstam-Vermutung (nämlich daß der Satz von Bombieri-Vinogradov mit dem vergrößerten Modulbereich $Q \leq x^{1-\delta}$ gilt), konnten sie ferner auch die bounded gap conjecture folgern, nämlich daß

$$\liminf_{n\to\infty} d_n \leq 16.$$

Die entscheidende Idee hierbei ist eine neue Siebmethode, die im wesentliche eine raffinierte Variante des Selberg-Siebs ist, das wir in §5 kennengelernt haben.

Inspiriert von diesen Ergebnissen über kleine Primzahllücken kann man auch Lücken zwischen aufeinanderfolgenden Goldbachzahlen betrachten, um wiederum Annäherungen an die binäre Goldbachvermutung zu gewinnen.
Seien dazu $4 = g_1 < g_2 < g_3 < \ldots$ die Goldbachzahlen, die Summe zweier Primzahlen sind. Betrachte dazu dann die größte Lücke bis zur Schranke X, also

$$A(X) := \max_{g_k \leq X}(g_{k+1} - g_k).$$

Damit ist die binäre Goldbachvermutung äquivalent zu der Aussage, daß $A(X) = 2$ für $X \geq 4$ ist.
2001 konnten Baker, Harman, Jia und Pintz zeigen, daß alle Intervalle vom Typ $[X, X + X^{21/800}]$ eine Goldbachzahl enthalten, d. h. es gilt

$$g_{n+1} - g_n \ll g_n^{21/800} \Leftrightarrow A(X) \ll X^{21/800}.$$

Kátai zeigte schon 1967, daß unter Annahme der RH folgt, daß

$$g_{n+1} - g_n \ll \log^2 g_n \Leftrightarrow A(X) \ll \log^2 X.$$

§ 7 Ein Nachwort zur Vorlesung – „apologies“

Die Auswahl des Vorlesungsstoffs war recht subjektiv inspiriert und betraf eher die analytische Richtung der additiven Zahlentheorie, denn aufgrund der Fülle mußte natürlich eine sehr enge Auswahl für die kurze Vorlesungszeit getroffen werden. Etwa zu der mehr kombinatorischen Richtung der additiven Zahlentheorie habe ich nicht allzuviel gesagt, konnte sie manchmal aber nicht unerwähnt lassen (z. B. Tao und Green).

Den geplanten §7 mußte ich fortlassen: Einen Überblick über den Beweis des Satzes von Chen zu geben, ist doch zu schwierig. Es wäre Stoff im Umfang einer etwa zweistündigen Vorlesung gewesen und sicher schön als ein Projekt für die Zukunft. Und andere Zukunftsprojekte gäbe es sicher auch noch...

An diejenigen HörerInnen, die die Vorlesung nach dem ersten Kapitel verlassen haben, weil sie die Konsequenzen der Riemannschen Vermutung über die Verteilung der Primzahlen für Science-Fiction hielten (ganz so war es natürlich nicht ☺): Um sich von diesen Konsequenzen wirklich zu überzeugen, müßte man eigentlich eine analytische Zahlentheorie gehört haben; ich habe mich nur darauf beschränkt, die für die weitere Vorlesung wichtigsten Ergebnisse zu nennen. Vielleicht ist es ja so, daß es nun manchen Hörer oder Hörerin nach dieser Vorlesung nicht mehr so wie früher überrascht, wenn sie von Konsequenzen aus der Gültigkeit der RH hören und können ihre Wichtigkeit nun besser einschätzen. (Jedenfalls war das eine Motivation für mich, analytische Zahlentheorie zu lernen.)

Was wollte ich? Zum einen wollte ich vermitteln, daß diese ZT-Richtung ein interessantes und sehr lebendiges aktuelles Forschungsgebiet ist, in dem sich gerade in letzter Zeit viele Neuerungen ergeben haben (nein, Zahlentheoretiker sind keine Orchideensammler...). Zum anderen wollte ich einen Einblick in die wichtigsten gängigen Methoden liefern und einen Grundstock des nötigen Handwerkzeugs vermitteln, der einen dazu in die Lage versetzt, vielleicht auch eigenständig in dem Gebiet weiterzuarbeiten. Ob ich diese hohen Ziele erreicht habe, weiß ich natürlich nicht, aber ich freue mich sehr, daß einige so großes Interesse für den Inhalt der Vorlesung gezeigt haben.

Kleine Hinweise zum Skript: Ich verwende gerne – meist gängige – Abkürzungen, die aber dort, wo sie zuerst auftauchen, erläutert sind (RH, GRH, PZS, AP, CM, CCM...). Das Zeichen (Ü) bezieht sich auf eine Übungsaufgabe, die besprochen wurde, und deren Ergebnis in den Vorlesungsstoff einfließt („Übungs-Smiley“). Das Zeichen Œ heißt ohne Einschränkung, und Verzeihung, daß ich der alten Rechtschreibung anhängig bin, weil mir die neue noch niemand beigebracht hat.

Literaturhinweise habe ich in den Text mit einfließen lassen, mit MathSciNet etc. sind diese ja leicht zu finden. Im wesentlichen habe ich einige Teile aus den Vorlesungen von Herrn Wolke übernommen, sowie Teile aus dem Buch von Nathanson [Melvyn B. Nathan-

son: Additive Number Theory - The Classical Bases. Graduate Texts in Mathematics 164, Springer 1996]. Das letzte Kapitel übernimmt einige Teile aus dem Übersichtsartikel von Kumchev und Tolev [A.V. Kumchev, D.I. Tolev: An Invitation to Additive Prime Number Theory. Serdica Math. J. 31 (2005), no. 1-2, 174].

Und nicht zuletzt vielen Dank an die Mitwirkenden: Meinem Tutor M. Molz für die exzellente Übungsbetreuung, Frau M. Gilg für das Schreiben der ersten LaTeX-Rohfassung des Online-Skripts und der Übungsblätter, und allen HörerInnen, die unermüdlich mitgearbeitet haben und dabei auch sehr verdeckte Fehler aufgedeckt haben. Durch die Fragen und Diskussionen haben alle sehr profitiert.

Karin Halupczok