Skriptum zur Vorlesung

Zahlentheorie II

Analytische Zahlentheorie

Sommersemester 2006

Prof. Dr. Helmut Maier
Dipl.-Math. Daniel Haase

Abteilung für Zahlentheorie und Wahrscheinlichkeitstheorie

Inhaltsverzeichnis

0. Grundlagen aus der Elementaren Zahlentheorie

Wir stellen zunächst einige Begriffe und Tatsachen aus der Elementaren Zahlentheorie - meist ohne Beweis - zusammen.

DEFINITION 0.0.1
Es seien $a, b \in \mathbb{Z}$, $a \neq 0$. b heißt durch a teilbar (a teilt b) genau dann, wenn es $x \in \mathbb{Z}$ gibt, so dass $ax = b$ ist. a heißt dann Teiler von b, b heißt Vielfaches von a. Wir schreiben $a|b$. Falls a nicht durch b teilbar ist, schreiben wir $a \nmid b$.

Wir stellen einige einfache Eigenschaften der Teilbarkeitsrelation zusammen:

SATZ 0.0.1
Es seien $a, b, c \in \mathbb{Z}$, dann gilt:

(i) $a|b \Rightarrow a|bc$,
(ii) $a|b$ *und* $b|c \Rightarrow a|c$,
(iii) $a|b$ *und* $a|c \Rightarrow a|(bx + cy)$ *für alle* $x, y \in \mathbb{Z}$,
(iv) $a|b$ *und* $b|a \Rightarrow a = \pm b$,
(v) $a|b$ *und* $a, b > 0 \Rightarrow a \leq b$,
(vi) *ist* $m \neq 0$, *so gilt* $a|b \Leftrightarrow ma|mb$.

SATZ 0.0.2 (Division mit Rest)
Es seien $a, b \in \mathbb{Z}$ mit $a > 0$ gegeben, dann gibt es eindeutig bestimmte Zahlen q und r, so dass $b = qa + r$ ist mit $0 \leq r < a$. Falls $a \nmid b$, so ist $0 < r < a$.

DEFINITION 0.0.2
Die ganze Zahl a heißt gemeinsamer Teiler von b und c, falls $a|b$ und $a|c$ gilt.

Da jede von 0 verschiedene Zahl nur endlich viele Teiler besitzt, gibt es nur endlich viele gemeinsame Teiler von b und c, außer im Fall $b = c = 0$. Falls es wenigstens eine Zahl b oder c ungleich 0 ist, heißt der größte ihrer gemeinsamen Teiler der größte gemeinsame Teiler von b und c, und wird mit $\mathrm{ggT}(b, c)$ oder kurz (b, c) bezeichnet. Der größte gemeinsame Teiler mehrerer Zahlen $a_1, \ldots, a_n$ wird mit $\mathrm{ggT}(a_1, \ldots, a_n)$ bezeichnet. Wir sagen a und b sind teilerfremd, falls $(a, b) = 1$ ist. Entsprechend nennt man $a_1, \ldots, a_n$ teilerfremd, wenn $\mathrm{ggT}(a_1, \ldots, a_n) = 1$ ist. Wir nennen $a_1, \ldots, a_n$ paarweise, falls $(a_i, a_j) = 1$ ist für $i \neq j$.

SATZ 0.0.3
Der größte gemeinsame Teiler (a, b) kann als ganzzahlige Linearkombination von a und b geschrieben werden, d. h. es gibt $x, y \in \mathbb{Z}$ mit $ax + by = (a, b)$.

Die Berechnung des ggT und der Koeffizienten geschieht mit Hilfe des Euklidischen Algorithmus, den wir im Folgenden erläutern. Er basiert auf den folgenden Eigenschaften des ggT:

LEMMA 0.0.4
Für alle $a, b \in \mathbb{Z}$ gilt $(a, b) = (b, a)$ und $(a, b) = (a, b - qa)$ für alle $q \in \mathbb{Z}$.

BEWEIS
Die erste Behauptung ist klar. Ist $q \in \mathbb{Z}$ beliebig und d irgend ein gemeinsamer Teiler von a und b, etwa $a = a'd$ und $b = b'd$, so gilt $b - qa = b'd - qa'd = d \cdot (b' - qa')$, d. h. d ist auch ein Teiler von a und $b - qa$ für alle $q \in \mathbb{Z}$. Teilt dagegen ein d die Zahlen a und $b - qa$, so auch $b - qa + qa = b$. Also stimmen die Teiler überein und damit auch deren Maximum, der ggT. □

Man kann den Euklidischen Algorithmus daher wie folgt beschreiben: die beiden Identitäten des Lemmas werden sukzessive angewendet, bis der Ausdruck (a, b) in die Form $(g, 0)$ gebracht wurde, woraus $(a, b) = (g, 0) = g$ folgt. Für eine übersichtliche Rechnung auf dem Papier bietet sich eine tabellarische

Notation der Rechenschritte an. Dazu tauscht man ggf. die Zahlen, so dass $a > b$ ist, und setzt $a_1 = a$ und $a_2 = b$. Danach wendet man sukzessive den Rekursionsschritt

$$a_n \ := \ a_{n-2} - q_n \cdot a_{n-1}$$

mit dem größtmöglichen $q_n = \lfloor \frac{a_{n-2}}{a_{n-1}} \rfloor$ an. Die definierende Eigenschaft der Division mit Rest ist es, dass der Betrag des Rests a_n stets kleiner ist als der Betrag des Divisors a_{n-1}, d. h. die Beträge der so konstruierten Folge sind streng monoton fallend, und nach endlich vielen Schritten ist $a_n = 0$. Das letzte nichttriviale Folgenglied ist dann der ggT.

Beispiel 0.0.1
Wir berechnen den ggT von 7 und 25. In der zugehörigen Tabelle werden der Übersicht halber die Reste a_n sowie die Quotienten q_n notiert:

n	$\mathbf{a_n}$	$\mathbf{q_n}$
1	25	
2	7	
3	4	3
4	3	1
5	$\boxed{1}$	1
6	0	3

Der Euklidische Algorithmus kann erweitert werden, so dass er auch die Koeffizienten $r, s \in \mathbb{Z}$ berechnet mit $ra+sb = (a, b)$. Die beiden Operationen „Tauschen“ und „Modulus abziehen“ können parallel zum ggT auch auf die Koeffizienten angewendet werden, es gilt dann in jedem Schritt der Rechnung, dass $ra + sb$ gerade der Rest der letzten Umformung ist, d. h. im vorletzten Schritt ist $ra + sb = (a, b)$. Die Werte der Koeffizienten werden wie die Reste als Folgen (r_n) und (s_n) aufgefasst und in der Tabelle mitgeführt, dabei sind in jedem Schritt die Werte r_n bzw. s_n als Reste mit dem Quotienten q_n zu berechnen:

$$\begin{aligned} r_n &:= r_{n-2} - q_n \cdot r_{n-1} \\ s_n &:= s_{n-2} - q_n \cdot s_{n-1} \end{aligned}$$

Der Quotient q_n stammt aus der Division mit Rest der (a_n)-Glieder des ursprünglichen Verfahrens. Es wird $r_1 = 1$ und $s_1 = 0$ gesetzt, damit im ersten Schritt $r_1a_1 + s_1a_2 = a_1$ gilt, bzw. $r_2 = 0$ und $s_2 = 1$, d. h. $r_2a_1 + s_2a_2 = a_2$. Wird die obige Rekursionsvorschrift angewendet, so gilt in jedem Schritt $r_na_1 + s_na_2 = a_n$ wie gewünscht. Für das vorige Beispiel ergibt sich die folgende Tabelle, in der die Koeffizienten r_n und s_n in jeder Zeile den Rest a_n aus den ursprünglichen Zahlen a und b kombinieren:

n	$\mathbf{a_n}$	$\mathbf{q_n}$	$\mathbf{r_n}$	$\mathbf{s_n}$
1	25		1	0
2	7		0	1
3	4	3	1	-3
4	3	1	-1	4
5	$\boxed{1}$	1	$\boxed{2}$	$\boxed{-7}$
6	0	3	-7	25

Daraus ergibt sich die Linearkombination des ggT zu $2 \cdot 25 + (-7) \cdot 7 = 1$.

Aus Satz 0.0.3 ergibt sich

Satz 0.0.5
Falls $c|ab$ und $(c, a) = 1$, so gilt $c|b$.

Beweis
Es seien $x, y \in \mathbb{Z}$ mit $cx + ay = 1$ und $ab = dc$ für ein $d \in \mathbb{Z}$. Dann gilt

$$cbx + aby \;=\; b \;\;\Rightarrow\;\; c(bx + dy) \;=\; b \;\;\Rightarrow\;\; c|b\,.$$

□

Wir erinnern an den Begriff der Primzahl: $p \in \mathbb{N}$ mit $p > 1$ ist eine Primzahl, wenn aus $d|p$ für $d > 1$ stets $d = p$ folgt. Aus Satz 0.0.5 folgt unmittelbar

Satz 0.0.6
Ist p eine Primzahl und gilt $p|ab$ für $a, b \in \mathbb{Z}$, so folgt $p|a$ oder $p|b$.

Aus Satz 0.0.6 lässt sich leicht der Fundamentalsatz der Arithmetik ableiten:

Satz 0.0.7
Jede natürliche Zahl $n > 1$ lässt sich eindeutig als Produkt von Primzahlpotenzen schreiben:

$$n \;=\; p_1^{\alpha_1} \cdots p_r^{\alpha_r} \;\;,\;\; p_1 < p_2 < \cdots < p_r \text{ Primzahlen} \;\;,\;\; \alpha_i \in \mathbb{N}\,.$$

Mittels der Division mit Rest ergibt sich eine Partition von $\mathbb{Z}$ der ganzen Zahlen in Äquivalenzklassen: Restklassen oder Kongruenzklassen genannt.

Definition 0.0.3
Es sei $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Wir sagen, a ist kongruent zu b modulo m genau dann, wenn $m|(b-a)$ gilt, und schreiben $a \equiv b \bmod m$ bzw. $a \not\equiv b \bmod m$ falls $m \nmid (b-a)$. Für die Menge aller b mit $a \equiv b \bmod m$ schreiben wir $a \bmod m$.

Man sieht leicht, dass $a \equiv b \bmod m$ genau dann gilt, wenn a und b bei Division durch m den gleichen Rest lassen, wenn es also $q_1, q_2, r \in \mathbb{Z}$ gibt mit $0 \le r < m$ und $a = q_1 m + r$ sowie $b = q_2 m + r$. Man erhält sofort

Satz 0.0.8
Es sei $m \in \mathbb{N}$. Es gibt genau m Restklassen modulo m, und zwar $0 \bmod m, 1 \bmod m, \ldots, (m-1) \bmod m$. Diese bilden eine Partition von $\mathbb{Z}$.

Definition 0.0.4
Es sei $m \in \mathbb{N}$. Die Menge der Restklassen mod m bezeichnen wir mit $\mathbb{Z}/m\mathbb{Z}$.

Die Kongruenzrelation ist eine Abschwächung der Gleichheitsrelation. Aus $a = b$ folgt $a \equiv b \bmod m$ für alle $m \in \mathbb{N}$. Mit Kongruenzen kann weitgehend so gerechnet werden wie mit Gleichungen. Der Grund dafür ist, dass jede Kongruenz als Gleichung zwischen Restklassen geschrieben werden kann, d. h. $a \equiv b \bmod m \Leftrightarrow a \bmod m = b \bmod m$, und dass sich gewisse algebraische Strukturen, die auf der Menge der ganzen Zahlen gegeben sind, auf die Menge der Restklassen mod m übertragbar sind. Wie $\mathbb{Z}$ bildet auch $\mathbb{Z}/m\mathbb{Z}$ einen Ring bzgl. Addition und Multiplikation der Restklassen:

Definition 0.0.5
Addition und Multiplikation zweier Restklassen sind definiert durch

$$(a \bmod m) \;+\; (b \bmod m) \;\;=\;\; (a+b) \bmod m \quad,\quad (a \bmod m) \cdot (b \bmod m) \;\;=\;\; (a \cdot b) \bmod m\,.$$

Man prüft leicht nach, dass die rechten Seiten nur von der Restklasse, nicht aber von den Repräsentanten a, b abhängen. Dadurch sind Addition und Multiplikation auf $\mathbb{Z}/m\mathbb{Z}$ wohldefiniert. Wie in jedem Ring können auch in $\mathbb{Z}/m\mathbb{Z}$ Gleichungen addiert und multipliziert werden. Dies gilt daher auch für Kongruenzen modulo m. $\mathbb{Z}/m\mathbb{Z}$ ist jedoch im Allgemeinen kein Körper, weshalb die Kürzungseigenschaft nicht allgemein gilt: aus $ab \equiv ac \bmod m$ folgt nicht $b \equiv c \bmod m$.

Beispiel 0.0.2
Es gilt $3 \cdot 2 \equiv 3 \cdot 5 \bmod 9$, aber nicht $2 \equiv 5 \bmod 9$. Die Restklasse 3 mod 9 besitzt kein multiplikatives Inverses, d. h. es gibt kein $x \in \mathbb{Z}$ mit $(3 \bmod 9) \cdot (x \bmod 9) = (1 \bmod 9)$.

Solche multiplikativen Inversen existieren jedoch stets für teilerfremde Restklassen:

DEFINITION 0.0.6
Es sei $m \in \mathbb{N}$. $a \bmod m$ heißt teilerfremde Restklasse, falls $(a, m) = 1$ ist.

Um die Wohldefiniertheit von 0.0.6 zu gewährleisten, muss gezeigt werden, dass die Bedingung $(a, m) = 1$ entweder für alle Elemente der Restklasse $a \bmod m$ erfüllt ist, oder für keines. Dies folgt aber sofort aus Lemma 0.0.4. Ist $(a, m) = 1$ und ist $ax + my = 1$ die Darstellung aus Satz 0.0.3, so ist die Inverse von $a \bmod m$ die Restklasse $x \bmod m$, oder in Kongruenzschreibweise $ax \equiv 1 \bmod m$.

BEISPIEL 0.0.3
Wir wollen $a = 25513$ modulo $m = 73685$ invertieren. Anwenden des erweiterten Algorithmus ergibt

n	$\mathbf{a_n}$	$\mathbf{q_n}$	$\mathbf{r_n}$	$\mathbf{s_n}$
1	73685		1	0
2	25513		0	1
3	22659	2	1	-2
4	2854	1	-1	3
5	2681	7	8	-23
6	173	1	-9	26
7	86	15	143	-413
8	1	2	-295	852
9	0	86	143	-413

Damit ist $(-295) \cdot 73685 + 852 \cdot 25513 \ = \ 1$, d. h. das Inverse von 25513 mod 73685 ist 852 mod 73685.

DEFINITION 0.0.7
Es sei $m \in \mathbb{N}$. Die Menge der zu m teilerfremden Restklassen bezeichnen wir mit $(\mathbb{Z}/m\mathbb{Z})^*$. Die Eulersche φ-Funktion ist definiert durch $\varphi(m) = \#\,(\mathbb{Z}/m\mathbb{Z})^*$.

Aus den vorigen Überlegungen ergibt sich

SATZ 0.0.9
Es sei $m \in \mathbb{N}$. Die Menge $(\mathbb{Z}/m\mathbb{Z})^*$ der teilerfremden Restklassen mod m bildet bzgl. der Multiplikation eine Gruppe.

Ist p eine Primzahl, so besteht $(\mathbb{Z}/p\mathbb{Z})^*$ aus allen von dem Nullelement $0 \bmod p$ verschiedenen Elementen von $\mathbb{Z}/p\mathbb{Z}$:

SATZ 0.0.10
Ist p eine Primzahl, so ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper mit p Elementen.

Wir fassen zusammen: Kongruenzen $ab \equiv ac \bmod m$ können stets zu $b \equiv c \bmod m$ gekürzt werden, wenn $(a, m) = 1$ ist. Ist $m = p$ eine Primzahl, so bedeutet ist $(p, m) = 1$ gleichbedeutend mit $p \nmid a$.

Wir kommen nun zum Chinesischen Restsatz. Ist m ein Produkt von zwei teilerfremden Faktoren $m = k \cdot l$ mit $(k, l) = 1$, so kann der Ring $\mathbb{Z}/m\mathbb{Z}$ als direktes Produkt der kleineren Ringe $\mathbb{Z}/k\mathbb{Z}$ und $\mathbb{Z}/l\mathbb{Z}$ und die Gruppe $(\mathbb{Z}/m\mathbb{Z})^*$ als direktes Produkt der kleineren Gruppen $(\mathbb{Z}/k\mathbb{Z})^*$ und $(\mathbb{Z}/l\mathbb{Z})^*$ dargestellt werden. Wir wollen diese Definition kurz skizzieren: unter dem direkten Produkt zweier algebraischer Strukturen (d. h. Mengen mit gewissen Operationen und Axiomen) versteht man das kartesische Produkt der Mengen, auf der die Operationen komponentenweise ausgeführt werden. Beispielsweise wird in einem direkten Produkt $G \times H$ von Gruppen komponentenweise multipliziert und invertiert:

$$(g_1, h_1) \cdot (g_2, g_2) \ = \ (g_1 \cdot g_2, h_1 \cdot h_2) \ , \ (g, h)^{-1} \ = \ (g^{-1}, h^{-1}) \, .$$

Das wohl bekannteste Beispiel ist $\mathbb{R}^n = \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{R}\}$ als direktes Produkt (bzw. direkte Summe) von Vektorräumen mit komponentenweiser Addition und Skalarmultiplikation. Bevor wir den Restsatz formulieren betrachten wir folgendes

Beispiel 0.0.4
Es sei $m = 35 = k \cdot l$ mit $k = 7$ und $l = 5$. Wir betrachten die Zuordnung

$$\Phi : \mathbb{Z}/35\mathbb{Z} \longrightarrow (\mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z}) \quad , \quad a \bmod 35 \longmapsto (a \bmod 7, a \bmod 5) .$$

Wie folgende Tabelle zeigt, ist Φ bijektiv:

$a \bmod 5$ \ $a \bmod 7$	0	1	2	3	4	5	6
0	0	15	30	10	25	5	20
1	21	1	16	31	11	26	6
2	7	22	2	17	32	12	27
3	28	8	23	3	18	33	13
4	14	29	9	24	4	19	34

Wir berechnen als Beispiel das Produkt $(13 \bmod 35) \cdot (19 \bmod 35)$:

$$\Phi(13 \bmod 35) \;=\; (6 \bmod 7, 3 \bmod 5) \quad , \quad \Phi(19 \bmod 35) \;=\; (5 \bmod 7, 4 \bmod 5) ,$$

und komponentenweises Rechnen ergibt

$$(6 \bmod 7, 3 \bmod 5) \cdot (5 \bmod 7, 4 \bmod 7) \;=\; (2 \bmod 7, 2 \bmod 5) .$$

Wir entnehmen der Tabelle das Resultat $(13 \bmod 35) \cdot (19 \bmod 35) = 2 \bmod 35$. Analog vermittelt die Abbildung Φ auch eine Bijektion von $(\mathbb{Z}/35\mathbb{Z})^*$ auf $(\mathbb{Z}/7\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$.

Satz 0.0.11 (Chinesischer Restsatz (über $\mathbb{Z}$))
Es seien $m_1, \ldots, m_r \in \mathbb{N}$ paarweise teilerfremd, $m = m_1 \cdots m_r$ und $a_1, \ldots, a_r \in \mathbb{Z}$. Dann besitzen die r Kongruenzen

$$x \;\equiv\; a_1 \bmod m_1 \;\;,\;\; x \;\equiv\; a_2 \bmod m_2 \;\;,\;\; \ldots \;\;,\;\; x \;\equiv\; a_r \bmod m_r$$

eine gemeinsame Lösung. Die Restklasse $x \bmod m$ ist eindeutig bestimmt. Es ist $(x \bmod m) \in (\mathbb{Z}/m\mathbb{Z})^*$ genau dann, wenn $(a_i \bmod m_i) \in (\mathbb{Z}/m_i\mathbb{Z})^*$ für $i = 1 \ldots r$ gilt.

Als Folgerung erhalten wir die Multiplikativität der Eulerschen φ-Funktion. Man überprüft leicht, dass für Primzahlpotenzen p^α ($\alpha \in \mathbb{N}$) gilt: $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1} \cdot (p-1)$. Es folgt

Satz 0.0.12
Die Eulersche φ-Funktion ist multiplikativ: $\varphi(m_1 \cdot m_2) = \varphi(m_1) \cdot \varphi(m_2)$ falls $(m_1, m_2) = 1$. Es gilt

$$\varphi(m) \;=\; m \cdot \prod_{\substack{p \text{ prim} \\ p \mid m}} \left(1 - \frac{1}{p}\right) .$$

Kongruenzen treten oft in Zusammenhang mit zyklischen Phänomenen auf. Bei der Definition der Tageszeit (auf Stunden gerundet) wird die Zeitgerade auf einen Kreis mit 24 Markierungszeichen „abgewickelt“, bei der Definition des Monats auf einen Kreis mit 12 Markierungszeichen. Beide Ideen haben ihren Grund in zyklischen Prozessen, die in der Natur tatsächlich ablaufen. Die Funktion, welche die Zahlengerade auf den Kreis abbildet, ist die komplexe Exponentialfunktion:

Definition 0.0.8
Wir schreiben $e(x) = e^{2\pi i x}$.

Für $t \in \mathbb{R}$ ist $e(t) = e^{2\pi i t} = \cos(2\pi t) + i \sin(2\pi t)$, e bildet also die Zahlengerade $\mathbb{R}$ auf den Einheitskreis $E = \{z \in \mathbb{C} \mid |z| = 1\}$ ab. Das Urbild von $z_0 = e(t_0) \in E$ ist die Restklasse mod 1

$$t_0 \bmod 1 \;:=\; t_0 + \mathbb{Z} \;=\; \{t \in \mathbb{R} \mid t = t_0 + m \;,\; m \in \mathbb{Z}\}$$

von t_0. Wenn wir die oben eingeführten Restklassen $l \bmod q$ als Urbilder erhalten wollen, verwenden wir die folgende Abbildung:

Definition 0.0.9
Für $q \in \mathbb{N}$ und $n \in \mathbb{Z}$ definieren wir

$$e_q(n) \;=\; e\left(\frac{q}{n}\right) \;=\; e^{\frac{2\pi i n}{q}} \,.$$

Die komplexe Zahl $\zeta_q = e_q(1)$ ist eine primitive q-te Einheitswurzel.

Die Abbildung e_q bildet $\mathbb{Z}$ auf die (zyklische) Gruppe $E_q = \{\zeta_q^n \mid n \in \mathbb{Z}\}$ der q-ten Einheitswurzeln ab. Die Funktionen e und e_q sind Beispiele für Gruppencharaktere.

Definition 0.0.10
Es seien $(G, \circ)$ und $(H, *)$ Gruppen mit den Verknüpfungen $\circ$ bzw. $*$. Eine Abbildung $\Phi : G \to H$ heißt Gruppenhomomorphismus, falls

$$\Phi(g_1 \circ g_2) \;=\; \Phi(g_1) * \Phi(g_2)$$

für alle $g_1, g_2 \in G$ gilt.

Beispiel 0.0.5
Die Abbildungen $e : \mathbb{R} \to E$ bzw. $e_q : \mathbb{Z} \to E_q$ sind Homomorphismen der Gruppen $(\mathbb{R}, +)$ bzw. $(\mathbb{Z}, +)$ auf die Gruppen $(E, \cdot)$ bzw. $(E_q, \cdot)$.

Diese Abbildungen sind auch Beispiele für Gruppencharaktere (oder kurz Charaktere). Da dieser Begriff zu seiner Definition topologische Konzepte benötigt, verzichten wir auf die genaue Definition. Es sei nur erwähnt, dass die Stetigkeit der Abbildung gefordert wird, und die Bildgruppe $(E, \cdot)$ ist. Charaktere spielen in der Zahlentheorie eine große Rolle. Auch die in der Riemannschen Zetafunktion vorkommende Abbildung

$$h_s : \mathbb{N} \to \mathbb{C} \,,\; n \mapsto n^s$$

kann zu einem Charakter erweitert werden:

$$h_s : \mathbb{Q}^+ \to \mathbb{C} \,,\; \frac{m}{n} \mapsto \left(\frac{m}{n}\right)^s$$

ist für festes s ein Charakter der Gruppe $(\mathbb{Q}^+, \cdot)$ mit $\mathbb{Q}^+ = \{r \in \mathbb{Q} \mid r > 0\}$. Charaktere der Gruppe $(\mathbb{Z}/m\mathbb{Z})^*$ sind als Dirichletcharaktere bekannt. Die Charaktere eines direkten Produkts $G \times H$ von Gruppen G und H lassen sich aus den Charakteren der Gruppen G und H gewinnen: es seien χ_G bzw. χ_H Charaktere von G bzw. H, dann ist

$$\chi : G \times H \to E \,,\; (g, h) \mapsto \chi_G(g) \cdot \chi_H(h)$$

ein Charakter von $G \times H$. Für $g_1, g_2 \in G$, $h_1, h_2 \in H$ ist nämlich

$$\chi(g_1 g_2, h_1 h_2) \;=\; \chi_G(g_1 g_2) \cdot \chi_H(h_1 h_2) \;=\; \chi_G(g_1)\chi_G(g_2)\chi_H(h_1)\chi_H(h_2) \;=\; \chi(g_1, h_1) \cdot \chi(g_2, h_2) \,.$$

Diese Tatsache ist in Zusammenhang mit dem Chinesischen Restsatz, also der Darstellung von $\mathbb{Z}/qr\mathbb{Z}$ bzw. $(\mathbb{Z}/qr\mathbb{Z})^*$ als direkte Produkte $(\mathbb{Z}/q\mathbb{Z}) \times (\mathbb{Z}/r\mathbb{Z})$ bzw. $(\mathbb{Z}/q\mathbb{Z})^* \times (\mathbb{Z}/r\mathbb{Z})^*$ auch in der Zahlentheorie von großer Bedeutung, und der Grund für die Multiplikativität von vielen Summenausdrücken, die Charaktere beinhalten.

Beispiel 0.0.6 (Multiplikativität der Ramanujan-Summe)
Es sei $q \in \mathbb{N}$ und $m \in \mathbb{Z}$. Die Ramanujan-Summe ist definiert als

$$c_q(m) \;=\; \sum_{\substack{1 \le n \le q \\ (n,q)=1}} e_q(m \cdot n) \,.$$

Ist $(m, q) = 1$, so durchläuft mit n auch das Produkt mn alle Restklassen in $(\mathbb{Z}/q\mathbb{Z})^*$, woraus $c_q(m) = c_q(1)$ folgt. Die Abbildung

$$(\mathbb{Z}/q\mathbb{Z})^* \times (\mathbb{Z}/r\mathbb{Z})^* \;\longrightarrow\; (\mathbb{Z}/qr\mathbb{Z})^* \quad,\quad (m \bmod q, n \bmod r) \;\longmapsto\; (rm + qn) \bmod qr$$

ist für $(q,r)=1$ eine Bijektion. In diesem Fall ist die Ramanujan-Summe wegen

$$c_q(1)\cdot c_r(1) \;=\; \sum_{\substack{1\le m\le q\\ 1\le n\le r\\ (m,q)=(n,r)=1}} e_q(m)e_r(n) \;=\; \sum_{\substack{1\le m\le q\\ 1\le n\le r\\ (m,q)=(n,r)=1}} e_{qr}(rm+qn) \;=\; c_{qr}(1)$$

multiplikativ. Man zeigt leicht, dass für Primzahlpotenzen $q=p^\gamma$

$$c_{p^\gamma}(1) \;=\; \begin{cases} 1 & \text{falls} \quad \gamma=0 \\ -1 & \text{falls} \quad \gamma=1 \\ 0 & \text{falls} \quad \gamma>1 \end{cases}$$

gilt. Aus der Multiplikativität folgt $c_q(1)=\mu(q)$.

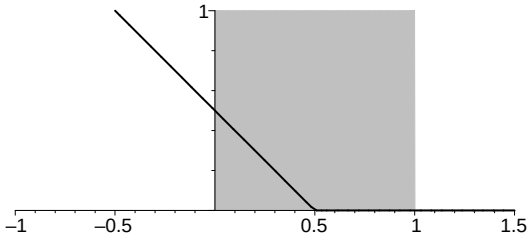
1. Weylsche Exponentialsummen

1.1. Einleitung

Exponentialsummen sind zentrale Objekte der analytischen Zahlentheorie. Im nächsten Kapitel werden wir sie verwenden, um ein scharfes Restglied im Primzahlsatz zu erhalten. Der entscheidende Bestandteil ist eine Abschätzung der Riemannschen Zetafunktion $\zeta(s)$ $(s = \sigma + it)$ in der Nähe von $\sigma = 1$ für $t \to \infty$. In vielen anderen Fragen der Primzahltheorie ist die Größenordnung der Riemannschen Zetafunktion im kritischen Streifen $\{0 < \sigma < 1\}$ von Bedeutung. In der Vorlesung Funktionentheorie II (Übungen, Aufgabe 33) hatten wir die μ-Funktion von Lindelöf eingeführt:

$$\mu(\sigma) \;=\; \inf\{\alpha \in \mathbb{R} \mid \zeta(\sigma + it) = O(t^\alpha)_{t\to\infty}\,,\ |t| \geq 1\}\,.$$

Außerdem wurde gezeigt, dass die so genannte Lindelöfsche Vermutung



$$\mu(\sigma) \;=\; \begin{cases} \frac{1}{2} - \sigma & \text{falls} \quad -\infty < \sigma \leq \frac{1}{2} \\ 0 & \text{falls} \qquad \sigma \geq \frac{1}{2} \end{cases}$$

aus der Riemannschen Vermutung folgt. Wir hatten einige Aussagen vollständig bewiesen (d. h. keine unbewiesenen Annahmen wie die Riemannsche Vermutung verwendet), beispielsweise

$$\zeta(s) \;=\; O(\log|t|)\ ,\ \ \zeta'(s) \;=\; O(\log^2|t|)\ \ (t\to\infty)\,,\ \sigma \;\geq\; 1 - c\cdot\log^{-1}|t|\,,$$

sowie $\mu(\frac{1}{2}) \leq \frac{1}{2}$, d. h. $\zeta(\frac{1}{2} + it) = O(t^{\frac{1}{2}+\varepsilon})$. Grundlegend für die Herleitung dieser Aussagen war die Approximation von $\zeta(s)$ im kritischen Streifen nach Hardy-Littlewood:

$$\zeta(s) \;=\; \sum_{n\leq t} n^{-s} \;-\; \frac{t^{1-s}}{1-s} \;+\; O(t^{-\sigma})\,.$$

Die Abschätzung $\mu(\frac{1}{2}) \leq \frac{1}{2}$ bzw. $\zeta(\frac{1}{2} + it) = O(t^{\frac{1}{2}+\varepsilon})$ ergibt sich durch die triviale Abschätzung der Summe

$$\sum_{n\leq t} n^{-s}\,.$$

Wir erinnern an Lemma 8.4.10 (Vorlesung Funktionentheorie II) zur abelschen Summation. Wegen seiner Wichtigkeit als elementare Technik formulieren wir es als unser erstes Lemma:

LEMMA 1.1.1 (Abelsche partielle Summation)
Es sei $f : [a, b] \to \mathbb{R}$ eine stetig-differenzierbare Funktion und $a < b$, sowie $c_1, c_2, \ldots$ komplexe Zahlen. Ist für $x \in [a, b]$

$$c(x) \;=\; \sum_{a<n\leq x} c_n\,,$$

so gilt

$$\sum_{a<n\leq b} c_n f(n) \;=\; -\int_a^b c(u)f'(u)du \;+\; c(b)f(b)\,.$$

Für die Summe über $n^{-(\frac{1}{2}+it)}$ erhalten wir damit

$$c(u) \;=\; \sum_{n\le u} n^{-it} \quad , \quad f(n) \;=\; n^{-\frac{1}{2}}$$

$$\Rightarrow \sum_{n\le t} n^{-\frac{1}{2}-it} \;=\; \sum_{\frac{1}{2}<n\le t} c_n f(n) \;=\; \frac{1}{2}\int\limits_{\frac{1}{2}}^{t} \left(\sum_{n\le u} n^{-it}\right) u^{-\frac{3}{2}} du \;+\; \left(\sum_{n\le t} n^{-it}\right) t^{-\frac{1}{2}}$$

mit $n^{-it} = |e^{-it\log(n)}| = 1$, wobei die triviale Abschätzung nach der Dreiecksungleichung

$$\left|\sum_{n\le u} n^{-it}\right| \;\le\; u$$

ergibt, und damit

$$\int\limits_{\frac{1}{2}}^{t} \left(\sum_{n\le u} n^{-it}\right) u^{-\frac{3}{2}} du \;\le\; \int\limits_{\frac{1}{2}}^{t} u^{-\frac{1}{2}} du \;=\; \left[2u^{\frac{1}{2}}\right]_{\frac{1}{2}}^{t} \;=\; 2t^{\frac{1}{2}} - \sqrt{2} \;\; , \;\; \left|\left(\sum_{n\le t} n^{-it}\right) t^{-\frac{1}{2}}\right| \;\le\; t\cdot t^{-\frac{1}{2}} \;=\; t^{\frac{1}{2}} \, .$$

Also $\zeta(\frac{1}{2}+it) = O(t^{\frac{1}{2}})$ bzw. $\mu(\frac{1}{2}) \le \frac{1}{2}$. Bei der Summe

$$\sum_{n\le u} n^{-it} \;=\; \sum_{n\le u} e^{-it\log(n)}$$

handelt es sich um eine Weylsche Exponentialsumme (oder auch trigonometrische Summe):

Definition 1.1.1
Wir schreiben $e(x) = e^{2\pi i x}$. Eine Weylsche Exponentialsumme oder trigonometrische Summe ist eine Summe der Form

$$\sum_{a<n\le b} e(f(n)) \, ,$$

wobei $f:\, [a,b] \to \mathbb{R}$ für $a < b$ eine stetig-differenzierbare Funktion ist.

Offenbar kann man $a, b \in \mathbb{Z}$ voraussetzen. Es ist bemerkenswert, dass der Wert von $e(f(n))$ nur vom gebrochenen Teil von $f(n)$ abhängt:

Definition 1.1.2
Für $x \in \mathbb{R}$ schreiben wir $x = [x] + \{x\}$ mit $[x] \in \mathbb{Z}$ und $\{x\} \in [0,1)$, und nennen $\{x\}$ den gebrochenen Teil von x.

Es bedeute $\|x\| := \min(\{x\}\,, 1-\{x\})$ den Abstand von x zur nächsten ganzen Zahl. Weylsche Exponentialsummen wurden erstmals von Hermann Weyl 1916 in seiner Arbeit „Über die Gleichverteilung von Zahlen mod. Eins“ eingeführt. Zerlegt man $f(n)$ als $f(n) = [f(n)] + \{f(n)\}$, so hängt wegen $e(f(n)) = e([f(n)]) \cdot e(\{f(n)\})$ mit $e([f(n)]) = 1$ der Wert von $e(f(n))$ nur vom gebrochenen Teil $\{f(n)\}$ von $f(n)$ ab.

Es ist nun zu erwarten, dass in einer Exponentialsumme

$$\sum_{a<n\le b} e(f(n)) \;=\; \sum_{a<n\le b} e(\{f(n)\}) \, ,$$

in der die Anzahl $b-a$ der Summanden genügend groß ist, für jedes nicht zu kurze Teilintervall $I:\, (\gamma,\delta) \subseteq (0,1)$ die Anzahl $N(I)$ der Terme $\{f(n)\} \in I$ etwa proportional zur Länge von I ist: $N(I) \sim (b-a)(\delta-\gamma)$. Nach dem Prinzip der Approximation des Riemannschen Integrals durch Riemannsche Summen sollte daher

$$\sum_{\substack{a<n\le b \\ \{f(n)\}\in I}} e(f(n))$$

den Ausdruck

$$(b-a)\cdot\int_I e(u)du$$

gut approximieren. Nun ist aber

$$\int_0^1 e(u)du \;=\; 0\,.$$

Es ist also zu erwarten, dass die Terme $e(f(n))$ auf dem Einheitskreis der komplexen Zahlenebene auf alle Richtungen „gleichverteilt“ sind, und sich somit weitgehend kompensieren. Der Betrag der Summe

$$\sum_{a<n\le b} e(f(n))$$

sollte also wesentlich kleiner als die triviale Schranke $b-a$ sein.

1.2. Exponentialsummen in Polynomen, Weylschritte

Eine der Ideen von Weyl war es, die Funktion $f(n)$ in der Exponentialsumme durch ein Taylorpolynom genügend hoher Ordnung zu approximieren. Damit kann das Problem der Abschätzung von

$$\sum_{a<n\le b} e(f(n))$$

auf den Fall zurückgeführt werden, dass $f(n)$ ein Polynom ist. Sind die Zahlen e_ν durch

$$\sum_{0<m\le b-a} e(f(a+m)) \;=\; \sum_{\nu=0}^{\infty} e_\nu \sum_{m=1}^{b-a} m^\nu e\left(f'(a)m+\cdots+\frac{f^{(k)}(a)}{k!}m^k\right)$$

gegeben, und ist e_ν für $\nu\ge 1$ genügend klein, so kann die Abschätzung der Exponentialsumme mittels partieller Summation auf die Abschätzung von Summen

$$\sum_{m=1}^{\mu} e(P(m))$$

mit dem Taylorpolynom

$$P_k(m) \;=\; f'(a)m \;+\; \cdots \;+\; \frac{f^{(k)}(a)}{k!}m^k$$

zurückgeführt werden. Wir werden im Folgenden Weyls Methode zur Abschätzung von Exponentialsummen der Form

$$\sum_{l=1}^{m} e(P(l))$$

mit einem Polynom P beschreiben. Die Idee ist, die Abschätzung von

$$\sum_{l=1}^{m} e(P_k(l))$$

mit einem Polynom k-ten Grades $P_k(l) = \alpha_k l^k + \alpha_{k-1}l^{k-1} + \cdots + \alpha_0$ durch einen so genannten Weylschritt auf die Abschätzung von Summen der Form

$$\sum_{l=1}^{m} e(P_{k-1}(l))$$

mit einem Polynom $(k-1)$-ten Grades zurückzuführen. Nach $(k-1)$ Schritten gelangt man schließlich zu einem linearen Polynom. Die zugehörigen Exponentialsummen sind endliche geometrische Reihen, deren Wert explizit bekannt ist. Formal wird der Beweis durch Induktion nach dem Grad des Polynoms

geführt. Die Qualität der Abschätzung hängt entscheidend von Diophantischen Approximationseigenschaften der Koeffizienten α_i von $P_k(x) = \alpha_k x^k + \alpha_{k-1}x^{k-1} + \cdots + \alpha_0$ ab.

Es gibt verschiedene Arten, die Güte einer Diophantischen Approximation einer reellen Zahl α durch eine rationale Zahl $\frac{p}{q}$ zu messen. Jedoch kann folgende Feststellung gemacht werden: von zwei Approximationen $\frac{p_1}{q_1}$ und $\frac{p_2}{q_2}$ (mit p_i, q_i jeweils teilerfremd) einer Zahl α ist, falls die Differenzen $|\alpha - \frac{p_1}{q_1}|$ und $|\alpha - \frac{p_2}{q_2}|$ etwa gleich groß sind, diejenige besser, für die der Nenner q_i deutlich kleiner ist.

Beispiel 1.2.1
Es ist $\pi = 3,14159265\ldots$, aus dieser Dezimalbruchentwicklung erhält man die Approximation

$$\frac{p_1}{q_1} \;=\; \frac{3141592}{1000000}$$

mit Differenz $\left|\pi - \frac{p_1}{q_1}\right| \approx 6 \cdot 10^{-7}$. Eine wesentlich bessere (weil einfachere) Approximation ist jedoch gegeben durch

$$\frac{p_2}{q_2} \;=\; \frac{355}{113}$$

mit $|\pi - \frac{p_2}{q_2}| \approx 6 \cdot 10^{-7}$.

Die reellen Zahlen, die die besten Diophantischen Approximationen gestatten, sind die ganzen Zahlen. Eine ganze Zahl $p \in \mathbb{Z}$ besitzt die Diophantische Approximation $\frac{p}{q}$ mit $q = 1$ und $p - \frac{p}{q} = 0$, d. h. Nenner und Differenz sind kleinstmöglich. Es sind jedoch gerade Polynome $P_k(x) = \alpha_k x^k + \cdots + \alpha_0$ mit ganzen Koeffizienten α_i, also Koeffizienten mit bestmöglichen Diophantischen Approximationseigenschaften, für die die triviale Abschätzung die richtige Größe liefert: Ist $\alpha_i \in \mathbb{Z}$, $1 \le i \le k$, so ist auch $P(n) \in \mathbb{Z}$ und damit $e(P(n)) = 1$ für alle $n \in \mathbb{Z}$. In der Exponentialsumme

$$\sum_{a<n\le b} e(P(n))$$

sind also die Terme $e(P(n))$ von der Gleichverteilung auf dem Einheitskreis maximal weit entfernt, und es ist

$$\sum_{a<n\le b} e(P(n)) \;=\; \sum_{a<n\le b} 1 \;=\; b - a\,.$$

Wir beginnen mit den linearen Polynomen:

Lemma 1.2.1
Es sei $\mu \in \mathbb{R}$ und $\lambda \in \mathbb{R}\backslash\mathbb{Z}$. Ist

$$S_1 \;=\; \sum_{n=a+1}^{b} e(\lambda n + \mu)\,,$$

so gilt

$$|S_1| \;\le\; \frac{1}{|\sin(\pi\lambda)|}\,.$$

Beweis
Nach der Summenformel für die endliche geometrische Reihe ist

$$|S_1| \;=\; \left|\frac{1 - e\left((b-a)\lambda\right)}{1 - e(\lambda)}\right| \;\le\; \frac{2}{|e(\frac{\lambda}{2}) - e(-\frac{\lambda}{2})|} \;=\; \frac{1}{|\sin(\pi\lambda)|}\,.$$

□

Bemerkung 1.2.1
Diese Abschätzung ist nur gut, d. h. wesentlich besser als die triviale Abschätzung $|S_1| \leq b-a$, falls $|\sin(\pi\lambda)|$ wesentlich größer als $(b-a)^{-1}$ ist, was wegen

$$\lim_{\lambda \to 0} \frac{\sin(\pi\lambda)}{\lambda} \;=\; \pi$$

bedeutet, dass $\|\lambda\|$ wesentlich größer als $(b-a)^{-1}$ ist.

Wir wenden uns nun dem allgemeinen Fall zu: Durch wiederholte Anwendung von Differenzenoperatoren wird das Polynom $P(n)$ durch Polynome kleineren Grades ersetzt:

Definition 1.2.1
Die Funktion f sei auf einer Teilmenge von $\mathbb{R}$ definiert, und es sei $d \in \mathbb{R}$. Wir setzen

$$\Delta_d(f)(x) \;:=\; f(x+d) - f(x)$$

für alle $x, d \in \mathbb{R}$, für welche die rechte Seite definiert ist. Für $l \geq 2$ ist der iterierte Differenzenoperator $\Delta_{d_l,d_{l-1},\ldots,d_1}$ rekursiv durch

$$\Delta_{d_l,d_{l-1},\ldots,d_1}(f)(x) \;=\; \Delta_{d_l}\left(\Delta_{d_{l-1},\ldots,d_1}(f)\right)(x)$$

gegeben.

Beispiel 1.2.2
Es ist

$$\begin{aligned}\Delta_{d_2,d_1}(f)(x) \;&=\; \Delta_{d_2}\left(\Delta_{d_1}(f)\right)(x) \;=\; \Delta_{d_1}(f)(x+d_2) - \Delta_{d_1}(f)(x)\\ &=\; f(x+d_2+d_1) - f(x+d_2) - f(x+d_1) + f(x)\,.\end{aligned}$$

Lemma 1.2.2
Es seien N_1, N_2 und N natürliche Zahlen, so dass $N_1 < N_2$ und $0 \leq N_2 - N_1 \leq N$ ist. Es sei $f(n)$ eine reellwertige zahlentheoretische Funktion und

$$S(f) \;=\; \sum_{n=N_1+1}^{N_2} e(f(n))\,.$$

Dann ist

$$|S(f)|^2 \;=\; \sum_{|d|\leq N} S_d(f) \;\text{ mit }\; S_d(f) \;=\; \sum_{n\in I(d)} e\left(\Delta_d(f)(n)\right)\,,$$

wobei $I(d)$ ein Intervall von aufeinander folgenden Zahlen ist, das in $[N_1+1, N_2]$ liegt.

Beweis
Für irgend eine Zahl d sei $I(d) = [N_1+1-d, N_2-d] \cap [N_1+1, N_2]$. Wir erhalten

$$|S(f)|^2 \;=\; S(f)\cdot\overline{S(f)} \;=\; \left(\sum_{m=N_1+1}^{N_2} e(f(m))\right)\cdot\left(\sum_{n=N_1+1}^{N_2} e(-f(n))\right)$$

$$= \sum_{n=N_1+1}^{N_2}\sum_{m=N_1+1}^{N_2} e\left((f(m)-f(n)\right) \;=\; \sum_{n=N_1+1}^{N_2}\sum_{d=N_1+1-n}^{N_2-n} e\left(f(n+d)-f(n)\right)$$

$$= \sum_{n=N_1+1}^{N_2}\sum_{d=N_1+1-n}^{N_2-n} e\left(\Delta_d(f)(n)\right) \;=\; \sum_{d=-(N_2-N_1-1)}^{N_2-N_1-1}\sum_{n\in I(d)} e\left(\Delta_d(f)(n)\right)$$

$$= \sum_{|d|\leq N}\sum_{n\in I(d)} e\left(\Delta_d(f)(n)\right) \;=\; \sum_{|d|\leq N} S_d(f)\,.$$

□

LEMMA 1.2.3
Es seien $N_1, N_2 \in \mathbb{N}$ und l eine ganze Zahl, so dass $l \geq 1$, $N_1 < N_2$ und $0 \leq N_2 - N_1 \leq N$ ist. Es sei $f(n)$ eine reellwertige zahlentheoretische Funktion und

$$S(f) \;=\; \sum_{n=N_1+1}^{N_2+1} e(f(n))\,.$$

Dann ist

$$|S(f)|^{2^l} \;\leq\; (2N+1)^{2^l-l-1} \sum_{|d_1|\leq N} \cdots \sum_{|d_l|\leq N} S_{d_l,\ldots,d_1}(f)$$

mit

$$S_{d_l,\ldots,d_1}(f) \;=\; \sum_{n\in I(d_l,\ldots,d_1)} e\left(\Delta_{d_l,\ldots,d_1}(f)(n)\right)\,,$$

wobei $I(d_l,\ldots,d_1)$ ein Intervall von aufeinander folgenden Zahlen ist, das in $[N_1+1, N_2]$ liegt.

BEWEIS
Der Beweis wird durch Induktion nach l geführt. Der Fall $l = 1$ ist gerade Lemma 1.2.2. Wir nehmen an, die Behauptung sei für $l \geq 1$ schon bewiesen. Mit der Cauchy-Schwarzschen Ungleichung folgt

$$|S(f)|^{2^{l+1}} \;=\; \left(|S(f)|^{2^l}\right)^2 \;\leq\; \left((2N+1)^{2^l-l-1} \sum_{|d_1|\leq N} \cdots \sum_{|d_l|\leq N} |S_{d_l,\ldots,d_1}(f)|\right)^2$$

$$=\; (2N)^{2^{l+1}-2l-2} \left(\sum_{|d_1|\leq N} \cdots \sum_{|d_l|\leq N} |S_{d_l,\ldots,d_1}(f)|\right)^2$$

$$\leq\; (2N)^{2^{l+1}-2l-2}(2N+1)^l \sum_{|d_1|\leq N} \cdots \sum_{|d_l|\leq N} |S_{d_l,\ldots,d_1}(f)|^2$$

mit

$$S_{d_l,\ldots,d_1}(f) \;=\; \sum_{n\in I(d_l,\ldots,d_1)} e\left(\Delta_{d_l,\ldots,d_1}(f)(n)\right)\,.$$

Nach Lemma 1.2.2 gibt es für jedes l-Tupel $(d_l,\ldots,d_1)$ ein Intervall

$$I(d_{l+1}, d_l, \ldots, d_1) \;\subseteq\; I(d_l,\ldots,d_1) \;\subseteq\; [N_1+1, N_2]$$

mit

$$|S_{d_l,\ldots,d_1}(f)|^2 \;=\; \left|\sum_{n\in I(d_l,\ldots,d_1)} e\left(\Delta_{d_l,\ldots,d_1}(f)(n)\right)\right|^2 \;=\; \sum_{|d_{l+1}|\leq N} \sum_{n\in I(d_{l+1},d_l,\ldots,d_1)} e\left(\Delta_{d_{l+1},d_l,\ldots,d_1}(f)(n)\right)$$

$$=\; \sum_{|d_{l+1}|\leq N} S_{d_{l+1},d_l,\ldots,d_1}(f)$$

und damit

$$|S(f)|^{2^{l+1}} \;\leq\; (2N+1)^{2^{l+1}-(l+1)-1} \sum_{|d_1|\leq N} \cdots \sum_{|d_{l+1}|\leq N} S_{d_{l+1},d_l,\ldots,d_1}(f)\,.$$

Damit ist Lemma 1.2.3 bewiesen. □

Wir wollen Lemma 1.2.3 nun auf $f(x) = P_k(x)$ mit $P_k(x) = \alpha_k x^k + \alpha_{k-1}x^{k-1} + \cdots + \alpha_0$ anwenden.

LEMMA 1.2.4
Es sei $k \in \mathbb{N}$ und $k \geq 2$, sowie $P_k(x) = \alpha_k x^k + \alpha_{k-1} x^{k-1} + \cdots + \alpha_0$ mit $\alpha_j \in \mathbb{R}$ und $d_1, d_2, \ldots, d_{k-1} \in \mathbb{Z}$. Dann gibt es ein $\beta \in \mathbb{R}$ mit

$$\Delta_{d_{k-1}, d_{k-2}, \ldots, d_1}(P_k)(x) \;=\; d_1 \cdots d_{k-1} \cdot k! \cdot \alpha_k x + \beta \,.$$

BEWEIS
Nach dem Binomischen Lehrsatz ist

$$P_k(x + d_1) \;=\; \alpha_k x^k + d_1 k \alpha_k x^{k-1} + \alpha_{k-1} x^{k-1} + Q_{k-2}(x)$$

mit einem Polynom $Q_{k-2}(x)$ vom Grad höchstens $k-2$. Also ist

$$\Delta_{d_1}(P_k)(x) \;=\; d_1 k \alpha_k x^{k-1} + R_{k-2}(x) \;\;,\;\; \deg(R_{k-2}) \leq k-2 \,.$$

Durch vollständige Induktion beweist man mit dieser Überlegung leicht für $l \leq k$

$$\Delta_{d_l, \ldots, d_1}(P_k)(x) \;=\; k(k-1)\cdots(k-l+1) \cdot d_l d_{l-1} \cdots d_1 \cdot \alpha_k x^{k-l} \;+\; R_{k-l-1} \,.$$

Diese Aussage liefert für $l = k-1$ und $R_0 = \beta$ das Ergebnis. □

SATZ 1.2.5
Es sei $P_k(x) = \alpha_k x^k + \alpha_{k-1} x^{k-1} + \cdots + \alpha_0$ mit $\alpha_i \in \mathbb{R}$, $k \geq 2$ und $K = 2^{k-1}$. Es sei $S = \sum e(P_k(n))$, wobei n über ein Intervall von höchstens N aufeinanderfolgenden Zahlen läuft. Dann gilt

$$|S|^K \;\leq\; 2^{3K} \cdot N^{K-1} + 2^{3K} \cdot N^{K-k} \cdot \sum_{1 \leq d_1, \ldots, d_{k-1} \leq N} \min\left(N, |\sin(\pi \alpha_k \cdot k! \cdot d_1 \cdots d_{k-1})|^{-1}\right) \,.$$

BEWEIS
Wir wenden Lemma 1.2.3 mit $l = k-1$ an, und erhalten mit Lemma 1.2.4

$$|S|^K \;\leq\; (2N+1)^{K-k} \cdot \Sigma_0 \tag{1}$$

mit

$$\Sigma_0 \;:=\; \sum_{|d_1| \leq N} \cdots \sum_{|d_{k-1}| \leq N} S_{d_{k-1}, \ldots, d_1}(P_k) \,,$$

$$S_{d_{k-1}, \ldots, d_1}(P_k) \;=\; \sum_{n \in I(d_{k-1}, \ldots, d_1)} e\left(\Delta_{d_{k-1}, \ldots, d_1}(P_k)(n)\right) \,,$$

wobei die $I(d_{k-1}, \ldots, d_1)$ Intervalle von Länge höchstens N sind. Wir spalten diese Summe auf:

$$\Sigma_0 \;=\; \Sigma_1 \;+\; \Sigma_2 \,. \tag{2}$$

In Σ_1 summieren wir über alle $(k-1)$-Tupel $(d_{k-1}, \ldots, d_1)$, für die alle $d_j \neq 0$ sind, in Σ_2 über die verbleibenden Tupel. Wir haben nach Lemma 1.2.4:

$$\Delta_{d_{k-1}, d_{k-2}, \ldots, d_1}(P_k)(x) \;=\; d_1 \cdots d_{k-1} \cdot k! \cdot \alpha_k x + \beta$$

und nach Lemma 1.2.1

$$|S_{d_{k-1}, \ldots, d_1}(P_k)| \;\leq\; \min\left(N, |\sin(\pi \alpha_k \cdot k! \cdot d_1 \cdots d_{k-1})|^{-1}\right)$$

In der Abbildung $\Phi : (d_{k-1}, \ldots, d_1) \longmapsto (|d_{k-1}|, \ldots, |d_1|)$ hat jedes Bild die 2^{k-1} paarweise verschiedenen Urbilder $(\pm|d_{k-1}|, \ldots, \pm|d_1|)$, daher gilt

$$|\Sigma_1| \;\leq\; 2^{k-1} \cdot \sum_{1 \leq d_1, \ldots, d_{k-1} \leq N} \min\left(N, |\sin(\pi \alpha_k \cdot k! \cdot d_1 \cdots d_{k-1})|^{-1}\right) \,. \tag{3}$$

Die Anzahl der $(d_{k-1}, \ldots, d_1)$ die mindestens eine Null enthalten, ist höchstens $(k-1) \cdot (2N+1)^{k-2}$. Daher gilt

$$|\Sigma_2| \;\leq\; (k-1) \cdot (2N+1)^{k-2} \cdot N \,.$$

Aus (1), (2) und (3) folgt

$$|S|^K \;\le\; (2N+1)^{K-k}(k-1)(2N+1)^{k-2}N$$
$$+ (2N+1)^{K-k}\cdot 2^{k-1} \;\cdot \sum_{1\le d_1,\ldots,d_{k-1}\le N} \min\left(N, |\sin(\pi\alpha_k\cdot k!\cdot d_1\cdots d_{k-1})|^{-1}\right) .$$

Die Behauptung folgt, wenn wir noch die Ungleichung $|k-1|\le 2^{k-1}$ benutzen. □

Satz 1.2.5 ist zentral in der Behandlung von Weylschen Exponentialsummen nach Weyl, Hardy und Littlewood. Da die Schranke entscheidend von der Diophantischen Natur des höchsten Koeffizienten α_k abhängt, kommen in den wichtigsten Anwendungen nicht ein festes Polynom, sondern - oft unendliche - Mengen von Polynomen vor. Es ist dann sicherzustellen, dass für die meisten dieser Polynome der höchste Koeffizient α_k günstige Eigenschaften hat, d. h. dass es nicht zu viele ganze Zahlen n gibt, für die $\|n\alpha_k\|$ klein ist. Eine Methode dies sicherzustellen besteht darin, eine rationale Approximation der Form

$$(*) \qquad \left|\alpha_k - \frac{a}{q}\right| \;\le\; \frac{1}{q^2}$$

vorauszusetzen, in welcher der Nenner q die passende Größenordnung besitzt. Die Verteilung der gebrochenen Teile $\{n\alpha_k\}$ ähnelt dann stark der Verteilung der $\{\frac{na}{q}\}$, die mit der Theorie der linearen Kongruenzen studiert werden kann. Daraus kann dann die so genannte Weylsche Ungleichung gefolgert werden.

Zunächst wollen wir uns einen Überblick über die Diophantischen Approximationen der Form $(*)$ verschaffen. Dies ist der Inhalt des Dirichletschen Approximationssatzes.

1.3. Der Dirichletsche Approximationssatz

Satz 1.3.1 (Dirichletscher Approximationssatz)
Es sei $N\in\mathbb{N}$ und $\alpha\in\mathbb{R}$. Dann gibt es $a\in\mathbb{Z}$ und $q\in\mathbb{N}$ mit $1\le q\le N$, so dass

$$\left|\alpha - \frac{a}{q}\right| \;\le\; \frac{1}{qN} .$$

Beweis
Jeder der gebrochenen Teile $\{0\},\{\alpha\},\{2\alpha\},\ldots,\{N\alpha\}$ liegt in einem der N Teilintervalle $[\frac{k}{N},\frac{k+1}{N}]$ für $0\le k\le N-1$. Nach dem Schubfachprinzip müssen mindestens zwei von ihnen, etwa $\{m_1\alpha\}$ und $\{m_2\alpha\}$ mit $m_1<m_2$, im selben Teilintervall liegen. Daher gilt

$$\left|\;\{m_2\alpha\}-\{m_1\alpha\}\;\right| \;\le\; \frac{1}{N}$$

und somit

$$(1) \qquad (m_2-m_1)\cdot\alpha \;=\; [m_2\alpha]-[m_1\alpha]+\{m_2\alpha\}-\{m_1\alpha\} .$$

Wir setzen $q=m_2-m_1$ und $a=[m_2\alpha]-[m_1\alpha]$. Wegen $0\le m_i\le N$ folgt $1\le q\le N$. Weiter folgt aus (1)

$$\alpha-\frac{[m_2\alpha]-[m_1\alpha]}{m_2-m_1} \;=\; \frac{\{m_2\alpha\}-\{m_1\alpha\}}{m_2-m_1}\text{, also } \left|\alpha-\frac{a}{q}\right| \;\le\; \frac{1}{qN} .$$

□

Satz 1.3.2
Ist α irrational, so gibt es unendlich viele rationale Zahlen $\frac{a}{q}$, so dass

$$\left|\alpha - \frac{a}{q}\right| \;\leq\; \frac{1}{q^2}$$

gilt.

Beweis
Wir konstruieren eine unendliche Folge von rationalen Zahlen $(\frac{a_i}{q_i})$ mit $a_i \in \mathbb{Z}$ und $q_i \in \mathbb{N}$, so dass

$$\left|\alpha - \frac{a_i}{q_i}\right| \;\leq\; \frac{1}{q_i^2} \tag{1}$$

und

$$\left|\alpha - \frac{a_{i+1}}{q_{i+1}}\right| \;<\; \left|\alpha - \frac{a_i}{q_i}\right| \quad \forall i \in \mathbb{N}\,. \tag{2}$$

Aus (2) folgt dann, dass die $\frac{a_i}{q_i}$ paarweise verschieden sind. Die Konstruktion verläuft rekursiv: wir setzen $q_1 = 1$ und $a_1 = [\alpha]$, dann ist offenbar (1) erfüllt. Es seien $\frac{a_1}{q_1}, \ldots, \frac{a_n}{q_n}$ bereits derart konstruiert, dass (1) und (2) gilt. Wir wählen $N_n \in \mathbb{N}$, so dass

$$\left|\alpha - \frac{a_n}{q_n}\right| \;>\; \frac{1}{N_n}\,. \tag{3}$$

Nach Satz 1.3.1 gibt es eine rationale Zahl $\frac{a_{n+1}}{q_{n+1}}$ mit $a_{n+1} \in \mathbb{Z}$, $q_{n+1} \in \mathbb{N}$ und $1 \leq q_{n+1} \leq N_n$, so dass

$$\left|\alpha - \frac{a_{n+1}}{q_{n+1}}\right| \;\leq\; \frac{1}{q_{n+1} \cdot N_n}\,, \tag{4}$$

also insbesondere

$$\left|\alpha - \frac{a_{n+1}}{q_{n+1}}\right| \;\leq\; \frac{1}{q_{n+1}^2}\,.$$

Aus (3) und (4) folgt überdies

$$\left|\alpha - \frac{a_{n+1}}{q_{n+1}}\right| \;<\; \left|\alpha - \frac{a_n}{q_n}\right|\,.$$

□

1.4. Die Teilerfunktion

Wir wollen zunächst die Summe aus Satz 1.2.5

$$\sum_{1 \leq d_1, \ldots, d_{k-1} \leq N} \min\left(N, |\sin(\pi\alpha_k \cdot k! \cdot d_1 \cdots d_{k-1})|^{-1}\right)$$

durch eine einfachere Summe von der Form

$$\sum_{n \leq M} \min\left(N, \|\alpha_k \cdot n\|^{-1}\right)$$

ersetzen. Dies geschieht dadurch, dass alle $(k-1)$-Tupel $(d_1, \ldots, d_{k-1})$, für die das Produkt $d_1 \cdots d_{k-1}$ einen festen Wert n annimmt, zusammengefasst werden. Es geht also zunächst darum, die Anzahl der Darstellungen der Form $d_1 \cdots d_{k-1} = n$ für $1 \leq d_i \leq N$, d. h. die Teilerfunktion abzuschätzen:

Definition 1.4.1
Die Teilerfunktion $\tau(n)$ ist definiert als die Anzahl der positiven Teiler von n:

$$\tau(n) \;=\; \left|\left\{\; (d_1,d_2) \mid d_1d_2 = n\;,\; d_1,d_2 \in \mathbb{N} \;\right\}\right| .$$

Die verallgemeinerte Teilerfunktion definieren wir für $k \in \mathbb{N}$ durch

$$\tau_k(n) \;=\; \left|\left\{\; (d_1,\ldots,d_k) \mid d_1\cdots d_k = n\;,\; d_1,\ldots,d_k \in \mathbb{N} \;\right\}\right| .$$

Es ist also $\tau(n) = \tau_2(n)$. In diesem Abschnitt sei die Primfaktorzerlegung von n stets $n = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$. Der Wert $\tau_k(n)$ hängt dann nur von den Exponenten α_i ab.

Lemma 1.4.1
Die Funktion $\tau_k(n)$ ist multiplikativ. Für Primzahlpotenzen gilt

$$\tau_k(p^\alpha) \;=\; \binom{\alpha+k-1}{k-1} .$$

Beweis
Jeder Zerlegung $n = d_1\cdots d_k$ entspricht das r-Tupel von Zerlegungen

$$p_j^{\alpha_j} \;=\; \mathrm{ggT}(d_1,p_j^{\alpha_j}) \cdot \cdots \cdot \mathrm{ggT}(d_k,p_j^{\alpha_j}) \;\;,\;\; 1 \le j \le r\,.$$

Die Zuordnung ist bijektiv, daher gilt mit

$$\tau_k(n) \;=\; \tau_k(p_1^{\alpha_1}) \cdot \cdots \cdot \tau_k(p_r^{\alpha_r})$$

die Multiplikativität. Der Wert $\tau_k(p^\alpha)$ ist gleich der Anzahl der Produktzerlegungen

$$p^\alpha \;=\; p^{\alpha_1}\cdots p^{\alpha_k} \;\;,\;\; \alpha_1+\cdots+\alpha_k \;=\; \alpha\,,$$

d. h. gleicht der Anzahl der Darstellungen von α als Summe von k nichtnegativen Summanden. Die Folgen $(\alpha_1,\ldots,\alpha_k)$ entsprechen umkehrbar eindeutig den Folgen $(\beta_1,\ldots,\beta_{k-1})$ mit

$$1 \;\le\; \beta_1 \;<\; \cdots \;<\; \beta_{k-1} \;\le\; \alpha+k-1\,,$$

wobei die Bijektion durch

$$\beta_j \;=\; (\alpha_1+1)+\cdots+(\alpha_j+1)$$

gegeben ist. Deren Anzahl ist gerade $\binom{\alpha+k-1}{k-1}$. □

Lemma 1.4.2
Es sei $\varepsilon > 0$ und $k \in \mathbb{N}$, dann ist $\tau_k(n) = O_{k,\varepsilon}\,(n^\varepsilon)$.

Bemerkung 1.4.1
Wir machen durch die Indizes k,ε deutlich, dass die im O-Symbol implizit vorhandene Konstante auch von k und ε abhängen darf. Der O-Ausdruck ist stets für $n \to \infty$ zu lesen. Bei komplizierten Ausdrücken benutzen wir anstelle des O-Symbols auch das Symbol $\ll$ bzw. $\ll_{k,\varepsilon}$.

Beweis von Lemma 1.4.2
Wir beweisen die Behauptung zunächst für $k = 2$: nach Lemma 1.4.1 ist $\tau(n) = (\alpha_1+1)\cdots(\alpha_r+1)$, deshalb ist

$$\frac{\tau(n)}{n^\varepsilon} \;=\; \frac{\alpha_1+1}{p_1^{\varepsilon\alpha_1}} \cdots \frac{\alpha_r+1}{p_r^{\varepsilon\alpha_r}}\,.$$

Für $p_s \le 2^{\frac{1}{\varepsilon}}$ haben wir

$$\frac{\alpha_s+1}{p_s^{\alpha_s}} \;\le\; \frac{\alpha_s+1}{2^{\varepsilon\alpha_s}} \;\le\; \frac{\alpha_s+1}{\varepsilon\alpha_s\log(2)} \;\le\; \frac{2}{\varepsilon\log(2)}\,,$$

daher ist

$$\frac{\tau(n)}{n^\varepsilon} \;\le\; \left(\frac{2}{\varepsilon\log(2)}\right)^{2^{\frac{1}{\varepsilon}}} .$$

Damit ist der Fall $k = 2$ bewiesen. Für den allgemeinen Fall führen wir eine Induktion nach k: aus der Darstellung $n = (d_1 \cdots d_{k-1}) \cdot d_k$ ergibt sich die Rekursion

$$\tau_k(n) \;=\; \sum_{d_k|n} \tau_{k-1}\left(\tfrac{n}{d_k}\right) \;\le\; \sum_{d_k|n} \tau_{k-1}(n) \;=\; \tau(n)\tau_{k-1}(n)\,.$$

□

1.5. Die Weylsche Ungleichung

LEMMA 1.5.1
Es sei $k \ge 1$, $K = 2^{k-1}$ und $\varepsilon > 0$. Es sei $P_k(x) = \alpha_k x^k + \cdots + \alpha_0$ mit $\alpha_i \in \mathbb{R}$. Wir setzen

$$S \;=\; \sum_{n=1}^{N} e\left(P_k(n)\right)\,,$$

dann gilt

$$|S|^K \;\underset{k,\varepsilon}{\ll}\; N^{K-1} \;+\; N^{K-k+\varepsilon} \sum_{m=1}^{k!N^{k-1}} \min\left(N, \|m\alpha_k\|^{-1}\right)\,.$$

BEWEIS
Wir verwenden die Abschätzung

$$\left|\sin\left(\pi\alpha_k k! d_1 \cdots d_{k-1}\right)\right|^{-1} \;=\; O\left(\|\alpha_k k! d_1 \cdots d_{k-1}\|^{-1}\right)$$

und sammeln für $1 \le n \le k!N^k$ alle $(k-1)$-Tupel $(d_1, \ldots, d_{k-1})$, für die $k! d_1 \cdots d_{k-1} = n$ ist. Nach Lemma 1.4.2 gibt es $O_{k,\varepsilon}(N^\varepsilon)$ solche $(k-1)$-Tupel, daraus folgt die Behauptung. □

Wir gehen nun daran, die Summe in Lemma 1.5.1 abzuschätzen:

LEMMA 1.5.2
Es sei $\alpha \in \mathbb{R}$, $q \ge 1$ und $(a, q) = 1$, sowie

$$\left|\alpha - \frac{a}{q}\right| \;\le\; \frac{1}{q^2}\,.$$

Dann gilt für $U, n \in \mathbb{R}$ die Abschätzung

$$\sum_{1 \le k \le U} \min\left(n, \frac{1}{\|\alpha k\|}\right) \;\ll\; \left(q + U + n + \frac{Un}{q}\right) \cdot \left(1 + \log(q)\right)\,.$$

BEWEIS
Es sei $\alpha = \frac{a}{q} + \frac{\theta}{q^2}$ mit $|\theta| \le 1$. Wir unterteilen das Intervall $[1, U]$ in höchstens $(\frac{U}{q} + 1)$ Teilintervalle $I_l := [U_l, U_{l+1}]$ der Länge $\le q$. Für ein festes l schätzen wir die Teilsumme

$$\Sigma_l \;:=\; \sum_{k \in I_l} \min\left(n, \frac{1}{\|\alpha k\|}\right)$$

ab. Zunächst schätzen wir für ein festes Paar (l, r) die Anzahl der $k \in I_l$ mit $\{k\alpha\} \in J_r := \left[\frac{r-1}{q}, \frac{r}{q}\right]$, $1 \le r \le q$ ab. Dazu seien $\{k_1\alpha\}, \{k_2\alpha\} \in J_r$ mit $k_1, k_2 \in I_l$. Es folgt

$$\left|\left\{\frac{k_2 a}{q}\right\} - \left\{\frac{k_1 a}{q}\right\}\right| \;\le\; \left|\{k_2\alpha\} - \{k_1\alpha\}\right| + |k_2 - k_1| \cdot \frac{1}{q^2} \;\le\; \frac{2}{q}\,.$$

Es gibt also höchstens 5 Werte k mit $\{k\alpha\} \in J_r$. Für $m \in \mathbb{N}$ ist daher

$$\left|\left\{k \in I_l \mid \|k\alpha\| \le \frac{m}{q}\right\}\right| \;\le\; 10m\,. \tag{1}$$

Wir zerlegen

$$\Sigma_l \;:=\; \sum_{k\in I_l} \min\left(n, \frac{1}{\|\alpha k\|}\right) \;=\; \Sigma_{l,1} \;+\; \Sigma_{l,2}\,, \tag{2}$$

wobei in $\Sigma_{l,1}$ über alle $k \in I_l$ mit $\min(n, \frac{1}{\|\alpha k\|}) = n$ summiert wird, und in $\Sigma_{l,2}$ über alle $k \in I_l$ mit $\min(n, \frac{1}{\|\alpha k\|}) = \frac{1}{\|\alpha k\|}$. Es gilt

$$\min\left(n, \frac{1}{\|\alpha k\|}\right) \;=\; n \;\Leftrightarrow\; \|\alpha k\| \;\leq\; \frac{1}{n} \;=\; \frac{q}{n}\cdot q^{-1}\,.$$

Die Anzahl dieser Terme ist $\ll \frac{q}{n} + 1$ nach (1). Damit ist

$$\Sigma_{l,1} \;\ll\; q + n\,. \tag{3}$$

Für $0 \leq s \leq \frac{\log(q)}{\log(2)}$ gibt es $\ll 2^s$ Werte $k \in I_l$ mit $\|k\alpha\| \leq 2^s q^{-1}$ wegen (1). Der Beitrag zur Summe $\Sigma_{l,2}$ ist $\ll \frac{2^s}{2^s q^{-1}} = q$. Summation über $0 \leq s \leq \frac{\log(q)}{\log(2)}$ ergibt

$$\Sigma_{l,2} \;\ll\; q\cdot(\log(q)+1)\,. \tag{4}$$

Aus (2), (3) und (4) erhalten wir

$$\Sigma_l \;\ll\; (q+n)\cdot(\log(q)+1)\,.$$

Summation über l ergibt

$$\sum_{1\leq k\leq U} \min\left(n, \frac{1}{\|k\alpha\|}\right) \;\ll\; (q+n)\cdot\left(\frac{U}{q}+1\right)\cdot(\log(q)+1) \;=\; \left(q+U+n+\frac{Un}{q}\right)\cdot(1+\log(q))\,,$$

und damit die Behauptung von Lemma 1.5.2. □

Satz 1.5.3 (Weylsche Ungleichung)
Es sei $P_k(x) = \alpha_k x^k + \cdots + \alpha_0$ mit $\alpha_i \in \mathbb{R}$ und $k \geq 1$, sowie

$$S \;=\; \sum_{n=1}^{N} e\left(P_k(n)\right) \;\;,\;\; \left|\alpha_k - \frac{a}{q}\right| \;\leq\; \frac{1}{q^2}\,.$$

Es sei $K = 2^{k-1}$ und $\varepsilon > 0$, dann ist

$$S \;\underset{k,\varepsilon}{\ll}\; N^{1+\varepsilon}\cdot\left(N^{-1}+q^{-1}+N^{-k}q\right)^{\frac{1}{K}}\,.$$

Beweis
Da $|S| \leq N$ ist folgt das Ergebnis sofort, falls $q \geq N^k$ ist. Wir können daher $1 \leq q \leq N^k$ annehmen, und damit $\log(q) \ll \log(N) \ll N^k$. Nach Lemma 1.5.1 ist

$$|S|^K \;\underset{k,\varepsilon}{\ll}\; N^{K-1} + N^{K-k+\varepsilon} \sum_{m=1}^{k!N^{k-1}} \min\left(N, \|m\alpha_k\|^{-1}\right)\,.$$

Nach Lemma 1.5.2 ist

$$\sum_{m=1}^{k!N^{k-1}} \min\left(N, \|m\alpha_k\|^{-1}\right) \;\ll\; \left(q + k!N^{k-1} + N + \frac{k!N^k}{q}\right)\cdot(1+\log(q))$$

$$\underset{k,\varepsilon}{\ll} \left(q + N^{k-1} + \frac{N^k}{q}\right)\cdot\log(N) \;\underset{k,\varepsilon}{\ll}\; N^k\cdot\left(qN^{-k}+N^{-1}+q^{-1}\right)\cdot N^{\varepsilon}\,.$$

Daher ist

$$|S|^K \;\underset{k,\varepsilon}{\ll}\; N^{K-1} + N^{K+\varepsilon}\cdot\left(qN^{-k}+N^{-1}+q^{-1}\right) \;\ll\; N^{K+\varepsilon}\cdot\left(qN^{-k}+N^{-1}+q^{-1}\right)\,.$$

□

1.6. Anwendungen und Beispiele

Die interessantesten Anwendungen der Weylschen Ungleichung ergeben sich im Zusammenhang mit der Kreismethode von Hardy und Littlewood. Wir wollen daher zunächst nur eine Anwendung dieser Ungleichung geben. Weiter diskutieren wir eine Anwendung des ursprünglichen Satzes 1.2.5.

1.6.1. *Polynome mit algebraischem höchsten Koeffizienten.*
Es sei $k \geq 2$, $P_k(x) = \alpha_k x^k + \cdots + \alpha_0$, $N \in \mathbb{N}$ und $\alpha_k = \sqrt[3]{2}$. Man gebe eine Abschätzung für

$$S \;=\; \sum_{n=1}^{N} e\left(P_k(n)\right)$$

mittels der Weylschen Ungleichung.

Lösung:
Wir benötigen zunächst eine Diophantische Approximation

$$\left|\alpha_k - \frac{a}{q}\right| \;\leq\; \frac{1}{q^2} \tag{1}$$

um die Weylsche Ungleichung

$$S \underset{k,\varepsilon}{\ll} N^{1+\varepsilon} \cdot \left(N^{-1} + q^{-1} + N^{-k}q\right)^{\frac{1}{K}} \tag{2}$$

mit $K = 2^{k-1}$ anwenden zu können. Die Terme q^{-1} und $N^{-k}q$ sind $\ll N^{-1}$ für den Bereich

$$N \;\ll\; q \;\ll\; N^{k-1}\,. \tag{3}$$

Falls wir ein q mit (1) und (3) finden können haben wir die Abschätzung

$$S \;\ll\; N^{1-\frac{1}{K}+\varepsilon}\,. \tag{4}$$

Wir werden im Folgenden zeigen, dass es ein solches q gibt.

Behauptung: Für $q \in \mathbb{N}$ und $a \in \mathbb{Z}$ ist stets

$$\left|\sqrt[3]{2} - \frac{a}{q}\right| \;\geq\; \frac{1}{10q^3}\,. \tag{5}$$

Beweis: Es sei $f(x) = x^3 - 2$, dann ist

$$f\left(\frac{a}{q}\right) \;=\; f\left(\sqrt[3]{2}\right) + f'(\theta) \cdot \left(\frac{a}{q} - \sqrt[3]{2}\right)$$

mit $f(\sqrt[3]{2}) = 0$ und θ zwischen $\sqrt[3]{2}$ und $\frac{a}{q}$. Es ist $1.2 \leq \sqrt[3]{2} \leq 1.3$. Man prüft die Gültigkeit von (5) leicht direkt für $1 \leq q \leq 4$. Es kann daher $q \geq 5$ und $0 \leq \theta \leq \frac{3}{2}$ und damit $|f'(\theta)| \leq 10$ angenommen werden. Nun ist $q^3 \cdot |f(\frac{a}{q})| = |a^3 - 2q^3| \geq 1$, also gilt

$$\left|\frac{a}{q} - \sqrt[3]{2}\right| \;\geq\; \frac{1}{|f'(\theta)|q^3} \;\geq\; \frac{1}{10q^3}$$

und damit (5).

Nach dem Dirichletschen Approximationssatz gibt es a, q mit $q = q(N)$ und $(a,q) = 1$, $1 \leq q \leq N^{k-1}$, so dass

$$\left|\frac{a}{q} - \sqrt[3]{2}\right| \;\leq\; \frac{1}{qN^{k-1}}\,.$$

Nach (5) muss aber $\frac{1}{qN^{k-1}} \geq \frac{1}{10q^3}$ sein, dies ergibt

$$\frac{1}{\sqrt{10}} N^{\frac{k-1}{2}} \;\leq\; q \;\leq\; N^{k-1}\,.$$

Es gilt also die Abschätzung (4): $S \ll N^{1-\frac{1}{K}+\varepsilon}$.

Überlegungen ähnlicher Art lassen sich für alle Fälle durchführen, in denen α_k algebraisch ist.

1.6.2. *Zetasummen.*
Wir betrachten nun die Zetasummen

$$\sum_{a<n\leq b} n^{-it}$$

die bei der Approximation und Abschätzung der Riemannschen ζ-Funktion eine Rolle spielen.

Lemma 1.6.1
Es sei $k \in \mathbb{N}$ und $t \geq 1$, $\frac{b-a}{a} \leq \frac{1}{2} t^{-\frac{1}{k+1}}$ und

$$\left| \sum_{m=1}^{\mu} \exp\left(-it \left(\frac{m}{a} - \frac{1}{2} \cdot \frac{m^2}{a^2} + \cdots + \frac{(-1)^{k-1} m^k}{k a^k} \right) \right) \right| \;\leq\; M \tag{1}$$

für alle $\mu \leq b-a$. Dann gilt

$$\left| \sum_{n=a+1}^{b} n^{-it} \right| \;\leq\; C \cdot M$$

mit einer absoluten Konstanten $C > 0$.

Beweis
Es ist

$$\Sigma \;:=\; \left| \sum_{n=a+1}^{b} e^{-it \cdot \log(n)} \right| \;=\; \left| \sum_{m=1}^{b-a} e^{-it \cdot \log(a+m)} \right|$$

$$= \left| \sum_{m=1}^{b-a} e^{-it \cdot \log(1+\frac{m}{a})} \right| \;=\; \left| \sum_{m=1}^{b-a} \exp\left(-it \cdot p_k\left(\frac{m}{a}\right) \right) \cdot \exp\left(-it \cdot q_k\left(\frac{m}{a}\right) \right) \right|$$

mit

$$p_k(u) \;=\; u - \frac{1}{2}u^2 + \cdots + \frac{(-1)^{k-1}}{k} u^k \;\;,\;\; q_k(u) \;=\; \sum_{l=k+1}^{\infty} \frac{(-1)^{l-1}}{l} u^l\,.$$

Weiter sei

$$r_k(u) \;=\; \sum_{l=k+1}^{\infty} \frac{u^l}{l}\,.$$

Die Funktionen $\exp(-it \cdot q_k(u))$ und $\exp(t \cdot r_k(u))$ besitzen für $|u| < 1$ konvergente Potenzreihenentwicklungen

$$\exp\left(-it \cdot q_k(u)\right) \;=\; \sum_{\nu=0}^{\infty} f_\nu(t) u^\nu \;\;,\;\; \exp\left(t \cdot r_k(u)\right) \;=\; \sum_{\nu=0}^{\infty} g_\nu(t) u^\nu\,.$$

Betrachtet man die Berechnungen der Koeffizienten $f_\nu(t)$ und $g_\nu(t)$, so ergibt ein Vergleich

$$|f_\nu(t)| \;\leq\; g_\nu(t)\,. \tag{2}$$

Wir erhalten

$$|\Sigma| \;=\; \left| \sum_{\nu=0}^{\infty} \frac{f_\nu(t)}{a^\nu} \sum_{m=1}^{b-a} m^\nu \exp\left(-it \cdot \left(\frac{m}{a} - \cdots + \frac{(-1)^{k-1} m^k}{k a^k} \right) \right) \right|\,.$$

Partielle Summation (Lemma 1.1.1) liefert:

$$\sum_{m=1}^{b-a} m^\nu e^{-it\cdot p_k\left(\frac{m}{a}\right)} \;=\; -\int_0^{b-a} \left(\sum_{m\le u} e^{-it\cdot p_k\left(\frac{m}{a}\right)}\right) \nu u^{\nu-1} du \;+\; (b-a)^{\nu-1} \sum_{m\le b-a} e^{-it\cdot p_k\left(\frac{m}{a}\right)},$$

und damit

$$|\Sigma| \;\le\; 2M \sum_{\nu=0}^{\infty} |f_\nu(t)| \cdot \left(\frac{b-a}{a}\right)^\nu$$

und wegen (2)

$$|\Sigma| \;\le\; 2M \cdot \exp\left(t\cdot \frac{(b-a)^{k+1}}{(k+1)a^{k+1}} + \cdots\right) \;\le\; 2M\cdot \exp\left(t\cdot \frac{\frac{(b-a)^{k+1}}{a^{k+1}}}{1-\frac{b-a}{a}}\right) \;\le\; 2M\cdot e^2\,.$$

□

Satz 1.6.2
Es sei $a \le b \le 2a$, $k \ge 2$, $K = 2^{k-1}$, $a \le ct$ und $t > t_0$. Dann ist

$$\Sigma \;=\; \sum_{n=a+1}^{b} n^{-it} \underset{k,c}{\ll} a^{1-\frac{1}{K}} \cdot t^{\frac{1}{(k+1)K}} \cdot \log^{\frac{1}{K}}(t) + a t^{-\frac{1}{(k+1)K}} \log^{\frac{k}{K}}(t)\,.$$

Beweis
Wir können $a \le 4t^{\frac{1}{k+1}}$ annehmen, da sonst die Abschätzung trivial ist. Wir setzen

$$\mu \;=\; \left[\frac{1}{2} a t^{-\frac{1}{k+1}}\right] \tag{1}$$

und $\Sigma = \Sigma_0 + \cdots + \Sigma_N$ mit

$$\Sigma_0 \;=\; \sum_{n=a+1}^{a+\mu} n^{-it} \;,\; \Sigma_\nu \;=\; \sum_{n=a+\nu\mu+1}^{a+\nu\mu+\mu} n^{-it}\,.$$

Nach Lemma 1.6.1 haben wir $\Sigma_\nu = O(M_\nu)$, wobei M_ν das Maximum über alle $\mu' \le \mu$ ist von

$$S_{\nu-1} \;=\; \sum_{m=1}^{\mu'} \exp\left(-it\cdot\left(\frac{m}{a+\nu\mu} - \frac{1}{2}\cdot\frac{m^2}{(a+\nu\mu)^2} + \cdots + (-1)^{k+1}\frac{m^k}{k(a+\nu\mu)^k}\right)\right)\,.$$

Nach Satz 1.2.5 haben wir

$$S_{\nu-1} \underset{k}{\ll} \mu^{1-\frac{1}{K}} + \mu^{1-\frac{k}{K}} \cdot \left(\sum_{1\le d_1,\ldots,d_{k-1}\le\mu} \min\left(\mu, \left|\sin\left(\frac{t(k-1)!\cdot d_1\cdots d_{k-1}}{2(a+\nu\mu)^k}\right)\right|^{-1}\right)\right)^{\frac{1}{K}}\,. \tag{2}$$

Es ist nun unmöglich, die rechte Seite von (2) für ein einzelnes ν gut abzuschätzen. Vielmehr müssen alle ν simultan betrachtet werden. Mit der Hölderschen Ungleichung erhalten wir

$$\Sigma \;\ll\; (N+1)\mu^{1-\frac{1}{K}} + \mu^{1-\frac{k}{K}} \cdot \sum_{\nu=0}^{N} \left(\sum_{1\le d_1,\ldots,d_{k-1}\le\mu} \min\left(\mu, \left|\sin\left(\frac{t(k-1)!\cdot d_1\cdots d_{k-1}}{2(a+\nu\mu)^k}\right)\right|^{-1}\right)\right)^{\frac{1}{K}}\,. \tag{3}$$

Wir setzen zur Abkürzung

$$h(\nu) \;=\; \frac{t(k-1)!\cdot d_1\cdots d_{k-1}}{2(a+\nu\mu)^k}\,. \tag{4}$$

Wegen

$$h'(\nu) \;=\; \frac{\mu\cdot t(k-1)!\cdot d_1\cdots d_{k-1}}{2(a+\nu\mu)^{k+1}}$$

liegt die „Schrittweite“ $h(\nu+1)-h(\nu)$ zwischen konstanten Vielfachen von $t(k-1)!d_1\cdots d_{k-1}\mu a^{-k-1}$, also wegen (1) von

$$(k-1)!\cdot d_1\cdots d_{k-1}\mu^{-k}\,. \tag{5}$$

Die Anzahl der Intervalle $I_l=\left[l-\frac{1}{2}\pi,l+\frac{1}{2}\pi\right]$, die Werte von $h(\nu)$ enthalten, ist daher

$$\ll\ (N+1)(k-1)!\cdot d_1\cdots d_{k-1}\mu^{-k}+1\,.$$

Wir schätzen für ein festes $(k-1)$-Tupel $(d_1,\ldots,d_{k-1})$ den Beitrag derjenigen Terme zur Summe in (3) ab, für die $h(\nu)$ in I_l liegt. Wir führen eine Zählung durch, die derjenigen im Beweis von Lemma 1.5.2 ähnelt. Für festes $s\le\log(t)$ gilt für die Anzahl $A(s)$ der Indices ν mit

$$|l\pi-h(\nu)|\ \le\ 2^s(k-1)!\cdot d_1\cdots d_{k-1}\mu^{-k}$$

die Abschätzung $A(s)=O(2^s)$. Daher ist der Beitrag nur

$$O\left(\frac{\mu^k\log(t)}{d_1\cdots d_{k-1}}\right)\,.$$

Die ν-Summe in (3) ist daher $\ll\ (N+1)\log(t)+\mu^k\log(t)^k$. Wenn wir über die $(k-1)$-Tupel $(d_1,\ldots,d_{k-1})$ summieren, erhalten wir

$$\Sigma\ \ll\ (N+1)\mu^{1-\frac{1}{K}}\ +\ (N+1)\mu^{1-\frac{1}{K}}\mu^{\frac{1}{K}}\ +\ t(N+1)^{1-\frac{1}{K}}\cdot\mu\cdot(\log^{\frac{k}{K}}(t))\,.$$

Wegen $N+1\ll\frac{b-a}{\mu}+1=O(t^{\frac{1}{K+1}})$ folgt die Behauptung. □

Beispiel 1.6.1
Wir wollen die Summe

$$\Sigma\ :=\ \sum_{a<n\le b}n^{-it}\quad\text{für } a\ =\ \left[\sqrt{t}\right]\ ,\ b\ =\ 2a$$

abschätzen. Wir wenden Satz 1.6.2 an mit $k=2$ und erhalten

$$\Sigma\ \ll\ a^{\frac{1}{2}}t^{\frac{1}{6}}\log^{\frac{1}{2}}(t)\ +\ at^{-\frac{1}{6}}\log(t)\ \underset{\varepsilon}{\ll}\ t^{\frac{5}{12}+\varepsilon}\,.$$

Satz 1.6.2 kann zusammen mit der Approximation nach Hardy-Littlewood

$$\zeta(s)\ =\ \sum_{n\le t}n^{-s}\ -\ \frac{t^{1-s}}{1-s}\ +\ O\left(t^{-\sigma}\right)\quad,\quad s=\sigma+it \tag{$*$}$$

dazu verwendet werden, die Größenordnung der Riemannschen ζ-Funktion im kritischen Streifen abzuschätzen. Es empfiehlt sich jedoch, insbesondere in der Nähe von $\sigma=\frac{1}{2}$, die approximative Funktionalgleichung der ζ-Funktion zu verwenden. Statt der „langen“ Zeta-Summe

$$\sum_{n\le t}n^{-s}$$

in $(*)$ enthält die approximative Funktionalgleichung die kürzeren Zeta-Summen

$$\sum_{n\le x}n^{-s}\ ,\ \sum_{n\le y}n^{-s}$$

mit $x\cdot y=t$. Die Methode zur Herleitung der approximativen Funktionalgleichung kann auch dazu verwendet werden, Weylsche Exponentialsummen abzuschätzen. Diese Methode geht auf van der Corput zurück.

1.7. Exponentialintegrale

Die zweite Hauptidee zur Abschätzung von Weylschen Exponentialsummen, die auf van der Corput zurückgeht, besteht darin, diese durch Exponentialintegrale abzuschätzen:

DEFINITION 1.7.1
Unter einem Exponentialintegral versteht man ein Integral der Form

$$\int_a^b g(x)e(f(x))dx\ ,$$

wobei f und g auf dem Intervall $[a,b]$ stetig-differenzierbar sind.

Der einfachste Fall ist wiederum der, in dem f ein lineares Polynom und $g(x)=1$ konstant ist. Hier lässt sich das Integral direkt auswerten. Dieser Fall liefert auch die Grundidee für die Behandlung des allgemeinen Falls. Es sei also $f(x)=\lambda_1 x+\lambda_0$ mit $\lambda_0,\lambda_1\in\mathbb{R}$ und $\lambda_1\neq 0$, dann ist

$$\int_a^b e(f(x))dx\ =\ \frac{1}{2\pi i\lambda_1}\left(e(\lambda_1 b+\lambda_0)-e(\lambda_1 a+\lambda_0)\right)\ . \tag{1.1}$$

Insbesondere ist

$$\int_a^b e(f(x))dx\ =\ O\left(\frac{1}{m}\right)\ ,$$

wobei m eine untere Schranke für die Größe der Ableitung $|f'(x)|$ ist: $|f'(x)|\geq m:=\lambda_1$. Die Größe der Ableitung $f'(x)$ misst die Schnelligkeit der Oszillation des Integranden $e(f(x))$. Die Funktion $e(\lambda_1 x+\lambda_0)$ hat die Periode $\frac{1}{|\lambda_1|}=\frac{2\pi}{|f'(x)|}$. Schnelle Oszillation des Integranden bewirkt einen kleinen Wert des Exponentialintegrals

$$\int_a^b e(f(x))dx\ .$$

Diese Beobachtung gilt auch für allgemeinere Situationen:

LEMMA 1.7.1
Es sei $a<b$ und $f,g:\ [a,b]\to\mathbb{R}$ stetig-differenzierbar auf $[a,b]$. Es sei $\frac{g(x)}{f'(x)}$ monoton auf $[a,b]$ und $\left|\frac{f'(x)}{g(x)}\right|\geq m>0$, dann gilt

$$\left|\int_a^b g(x)e(f(x))dx\right|\ \leq\ \frac{6}{m}\ . \tag{1}$$

BEWEIS
Wir behandeln (1) zunächst für den Spezialfall $f(x)=x$ und schätzen

$$\int_a^b g(x)e(x)dx$$

mit g monoton und stetig-differenzierbar ab. Partielle Integration ergibt

$$\int_a^b g(x)e(x)dx\ =\ g(b)\left(\int_a^b e(x)dx\right)-\int_a^b g'(x)\left(\int_a^x e(u)du\right)dx\ \leq\ 2|g(b)|+2(|g(a)|+|g(b)|)\ \leq\ \frac{6}{m}. \tag{2}$$

Im allgemeinen Fall substituieren wir $u = f(x)$ und definieren α, β durch $f(a) = \alpha$ und $f(b) = \beta$. Es sei $f^{-1}(u)$ die Umkehrfunktion von f. Wegen

$$\frac{df^{-1}(u)}{du} \;=\; \frac{1}{f'(f(u))}$$

erhalten wir aus (2)

$$\int_a^b g(x)e(f(x))dx \;=\; \int_\alpha^\beta e(u)\frac{g(f^{-1}(u))}{f'(f^{-1}(u))}du \;\leq\; \frac{6}{m}\,.$$

□

Als nächstes betrachten wir die Möglichkeit, dass die Ableitung $f'(x)$ im Exponentialintegral in einem Punkt c des Integrationsbereichs verschwindet: $f'(c) = 0$. Man sagt dann auch: $e(f(x))$ besitzt in $x = c$ eine stationäre Phase. Grob gesagt ist c ein Punkt, in dessen unmittelbarer Umgebung $e(f(x))$ nicht oszilliert.

Lemma 1.7.2
Es sei $a < b$ und $g : [a, b] \to \mathbb{R}$ stetig differenzierbar sowie $f : [a, b] \to \mathbb{R}$ zweimal stetig-differenzierbar. Auf $[a, b]$ sei $\frac{g(x)}{f'(x)}$ monoton und $|g(x)| \leq M$ sowie $|f''(x)| \geq r$. Dann ist

$$\left|\int_a^b g(x)e(f(x))dx\right| \;<\; \frac{12M}{\sqrt{r}}\,.$$

Beweis
Wegen $e(-f(x)) = \overline{e(f(x))}$ genügt es, sich auf den Fall $f''(x) \geq r > 0$ zu beschränken. Dann ist $f'(x)$ auf $[a, b]$ monoton wachsend. Es gibt dann höchstens einen Punkt $c \in [a, b]$ mit $f'(c) = 0$. In diesem Fall setzen wir $c_0 = c$. Falls $f'(x) > 0$ ist für alle $x \in [a, b]$ setzen wir $c_0 = a$, falls $f'(x) < 0$ für alle $x \in [a, b]$ ist setzen wir $c_0 = b$. Für $\delta > 0$ sei $c_1(\delta) = \max(a, c_0 - \delta)$ sowie $c_2(\delta) = \min(b, c_0 + \delta)$. Wir zerlegen das Exponentialintegral zu

$$\int_a^b g(x)e(f(x))dx \;=\; I_1 + I_2 + I_3$$

mit

$$I_1 \;=\; \int_a^{c_1(\delta)} g(x)e(f(x))dx \;\;,\;\; I_2 \;=\; \int_{c_1(\delta)}^{c_2(\delta)} g(x)e(f(x))dx \;\;,\;\; I_3 \;=\; \int_{c_2(\delta)}^{b} g(x)e(f(x))dx$$

und bestimmen $\delta > 0$ später. In I_1 und I_3 oszilliert $e(f(x))$ stark, in I_2 bzw. der Umgebung der stationären Phase dagegen schwach. Ist $c_1(\delta) = a$, so ist $I_1 = 0$. Andernfalls ist für $x \in [a, c_1(\delta)]$

$$|f'(x)| \;\geq\; \int_{c-\delta}^{c} |f''(x)|dx \;>\; \delta \cdot r\,.$$

Nach Lemma 1.7.1 ist dann $|I_1| \leq \frac{6M}{\delta r}$. Eine analoge Abschätzung ergibt $|I_3| \leq \frac{6M}{\delta r}$. Schließlich wird I_2 trivial abgeschätzt: $|I_2| \leq 2\delta M$. Insgesamt erhalten wir

$$\left|\int_a^b g(x)e(f(x))dx\right| \;\leq\; \frac{12M}{\delta r} \;+\; 2\delta M\,.$$

Wir wählen δ so, dass beide Terme gleich groß sind:

$$\delta \;=\; \frac{\sqrt{6}}{\sqrt{r}}\,.$$

Dafür erhalten wir

$$\left| \int_a^b g(x)e(f(x))dx \right| \ \leq \ \frac{4\sqrt{6}}{\sqrt{r}} M \ < \ \frac{12M}{\sqrt{r}} \, .$$

□

Es ist auch möglich, unter gewissen Bedingungen ein Exponentialintegral mit stationärer Phase asymptotisch auszuwerten. Da wir diese Resultate im Folgenden nicht benötigen, begnügen wir uns mit einer Beweisskizze:

LEMMA 1.7.3
Es sei $f : [a,b] \to \mathbb{R}$ *dreimal differenzierbar auf* (a,b). *Auf* (a,b) *gelte mit* $C > 0$

$$0 < \lambda_2 < f''(x) < C\lambda_2 \ , \ |f'''(x)| \leq C\lambda_3 \, .$$

Es sei $f'(c) = 0$ *mit* $a \leq c \leq b$. *Dann gilt*

$$\int_a^b e(f(x))dx \ = \ \frac{e^{\frac{1}{4}\pi i + 2\pi i f(c)}}{(f''(c))^{\frac{1}{2}}} + O_C\left(\lambda_2^{-\frac{4}{5}}\lambda_3^{\frac{1}{5}}\right) + O_C\left(\min(|f'(a)|^{-1}, \lambda_2^{-\frac{1}{2}})\right) + O_C\left(\min(|f'(b)|^{-1}, \lambda_2^{-\frac{1}{2}})\right) .$$

BEWEIS (SKIZZE)
Wie im Beweis von Lemma 1.7.2 spalten wir den Integrationsbereich auf:

$$\int_a^b e(f(x))dx \ = \ \int_a^{c-\delta} + \int_{c-\delta}^{c+\delta} + \int_{c+\delta}^b \, .$$

Das erste und das dritte Integral, in denen $e(f(x))$ stark oszilliert, werden mittels Lemma 1.7.1 abgeschätzt. Approximation von $f(x)$ nach dem Satz von Taylor führt zu

$$\int_{c-\delta}^{c+\delta} e(f(x))dx \ = \ e(f(c)) \int_{c-\delta}^{c+\delta} e\left(\frac{1}{2}(x-c)^2 f''(c)\left(1 + O\left((x-c)^3\lambda_3\right)\right)\right) dx \, .$$

Das Integral

$$\int_{c-\delta}^{c+\delta} e\left(\frac{1}{2}(x-c)^2 f''(c)\right) dx$$

wird mit dem uneigentlichen Integral

$$\int_{-\infty}^{\infty} e\left(\frac{1}{2}(x-c)^2 f''(c)\right) dx$$

verglichen, dessen Wert mittels komplexer Integration bestimmt werden kann. □

1.8. Methode von van der Corput und die approximative Funktionalgleichung

Wir kommen nun zum zentralen Satz, der Exponentialsummen mit Summen über Exponentialintegrale vergleicht. Wegen wichtiger Anwendungen wollen wir etwas allgemeinere Summen der Form

$$\sum_{a < n \leq b} g(n)e(f(n))$$

betrachten, in denen g eine stetig-differenzierbare Funktion ist. Die Grundidee ist die Anwendung der Poissonschen Summenformel

$$\sum_{n \in \mathbb{Z}} \Phi(n) \ = \ \sum_{n \in \mathbb{Z}} \hat{\Phi}(n)$$

mit der Fouriertransformierten

$$\hat{\Phi}(n) \;=\; \int\limits_{-\infty}^{\infty} \Phi(u)e(-nu)du\,,$$

von Φ auf die Funktion

$$\Phi(u) \;=\; \begin{cases} g(u)e(f(u)) & \text{falls} \quad a < u \leq b \\ 0 & \text{sonst} \end{cases}.$$

Unser Vorgehen wird viel mit dem Beweis der Poissonschen Summenformel (Aufgabe 22 aus Funktionentheorie II) gemeinsam haben.

Satz 1.8.1
Es sei $a < b$ und $f : [a,b] \to \mathbb{R}$ stetig-differenzierbar mit monotoner Ableitung $f'(x)$. $g : [a,b] \to \mathbb{R}$ sei positiv, monoton fallend und stetig-differenzierbar, so dass $|g'(x)|$ monoton fallend ist. Ist $\alpha = f'(b)$ und $\beta = f'(a)$, so gilt

$$(1)\quad \sum_{a<n\leq b} g(n)e(f(n)) \;=\; \sum_{\alpha-\eta<\nu\leq\beta+\eta} \int\limits_a^b g(x)e(f(x)-\nu x)dx \;+\; O\left(g(a)\cdot\log(\beta-\alpha+2)\right) \;+\; O(|g'(a)|)$$

mit einer beliebigen Konstanten $0 < \eta < 1$.

Bemerkung 1.8.1
Die Summationsbedingung $\alpha - \eta < \nu \leq \beta + \eta$ besagt, dass die stationäre Phase des Integrals

$$\int\limits_a^b g(x)e(f(x)-\nu x)dx$$

ins Innere des Intervalls (a,b) fällt (oder nicht weit davon entfernt ist):

$$\exists x_\nu \in (a,b) : \frac{d}{dx}(f(x_\nu)-\nu x_\nu) = 0 \quad\Leftrightarrow\quad \exists x_\nu \in (a,b) : f'(x_\nu) = \nu \quad\Leftrightarrow\quad \alpha = f'(b) \leq \nu \leq f'(a) = \beta$$

da f' stetig und monoton fallend ist.

Beweis von Satz 1.8.1
Wir können $\beta - \alpha \geq 10$ annehmen, zudem ist ohne Einschränkung $a = m_1 + \frac{1}{2}$ und $b = m_2 + \frac{1}{2}$ für $m_1, m_2 \in \mathbb{Z}$. Es sei nämlich $(\tilde{a}, \tilde{b})$ das größte in (a,b) enthaltene Teilintervall von der Form $(m_1 + \frac{1}{2}, m_2 + \frac{1}{2})$: wegen

$$\sum_{\alpha-\eta<\nu\leq\beta+\eta} e(f(t)-\nu t) \;\ll\; (\beta-\alpha+2) + \frac{1}{\|t\|}$$

ändert sich die rechte Seite von (1) höchstens um

$$O\left(g(a)\cdot\left(\int\limits_0^{(\beta-\alpha+2)^{-1}} (\beta-\alpha+2)dt \;+\; \int\limits_{(\beta-\alpha+2)^{-1}}^{\frac{1}{2}} \frac{1}{t}dt\right)\right) \;=\; O\left(g(a)\cdot\log(\beta-\alpha+2)\right).$$

Die linke Seite von (1) ändert sich um $O(g(a))$. Indem wir $f(x)$ gegebenenfalls durch $h(x) = f(x) - kx$ für $k \in \mathbb{Z}$ ersetzen, können wir zudem annehmen, dass $\eta - 1 < \alpha \leq \eta$ ist. Wir erinnern an folgende Sätze und Definitionen aus der Vorlesung Funktionentheorie II. Nach Definition 2.0.1 (Zusatzinhalte zu Funktionentheorie II) sind Dirichletkern D_n und Féjèrkern F_n gegeben durch

$$D_N(x) \;=\; \sum_{k=-N}^{N} e(kx) \quad,\quad F_N(x) \;=\; \frac{1}{2N+1}\sum_{k=-N}^{N} D_k(x)\,.$$

Nach Satz 2.0.4 (Zusatzinhalte zu Funktionentheorie II) gilt für $\Phi : \mathbb{R} \to \mathbb{C}$ stetig

$$\lim_{N\to\infty} \int_{n-\frac{1}{2}}^{n+\frac{1}{2}} \Phi(t) F_N(t) dt \;=\; \Phi(n) \tag{2}$$

für alle $n \in \mathbb{Z}$. Es ist klar, dass (2) auch schon gilt, wenn Φ auf $[n-\frac{1}{2}, n+\frac{1}{2}]$ stetig ist. Wir wenden (2) an mit

$$\Phi(t) \;=\; \begin{cases} g(t)e(f(t)) & \text{falls} \quad a \le t \le b \\ 0 & \text{sonst} \end{cases}$$

und erhalten

$$\sum_{a<n\le b} g(n)e(f(n)) \;=\; \lim_{N\to\infty} \frac{1}{2N+1} \sum_{k=-N}^{N} \sum_{\nu=-k}^{k} \int_a^b g(t)e(f(t)-\nu t)dt\,. \tag{3}$$

Es sei $I = (\alpha-\eta, \beta+\eta)$. Wir schätzen die Summe

$$\sum_{\substack{\nu=-k \\ \nu\notin I}}^{k} \int_a^b g(t)e(f(t)-\nu t)dt$$

ab. Wir haben

$$\int_a^b g(t)e(f(t)-\nu t)dt \;=\; \frac{1}{2\pi i}\left(J_1(\nu) - J_2(\nu)\right) \tag{4}$$

mit

$$J_1(\nu) \;:=\; \int_a^b \frac{1}{f'(t)-\nu} \cdot \frac{d}{dt}\left(g(t)e(f(t)-\nu t)\right) dt \;\;,\;\; J_2(\nu) \;:=\; \int_a^b \frac{g'(t)}{f'(t)-\nu} \cdot e\left(f(t)-\nu t\right) dt\,.$$

Wegen $e(\nu a) = e(\nu b) = (-1)^\nu$ und der Monotonie von $f'(x) - \nu$ haben wir für $\nu \notin I$

$$J_1(\nu) \;=\; \left[g(t)\frac{e(f(t)-\nu t)}{f'(t)-\nu}\right]_a^b \;-\; \int_a^b g(t)e(f(t)-\nu t) \cdot \frac{d}{dt}\left(\frac{1}{f'(t)-\nu}\right) dt$$

$$=\; \frac{(-1)^{\nu+1}}{\alpha-\nu} g(b) \;-\; \frac{(-1)^{\nu+1}}{\beta-\nu} g(a) \;+\; O\left(g(a) \cdot \left|\frac{1}{\alpha-\nu} - \frac{1}{\beta-\nu}\right|\right)\,.$$

Wir teilen die Summe

$$\sum_{\substack{n=-k \\ \nu\notin I}}^{k} J_1(\nu) \;=\; \Sigma_1 \;+\; \Sigma_2$$

auf mit

$$\Sigma_1 \;:=\; \sum_{\substack{\nu=-k \\ \nu\notin I \\ |\nu|\le 4(\beta-\alpha)}}^{k} J_1(\nu) \;\;,\;\; \Sigma_2 \;:=\; \sum_{\substack{\nu=-k \\ \nu\notin I \\ |\nu|> 4(\beta-\alpha)}}^{k} J_1(\nu)\,.$$

Die alternierenden Summen $\sum \frac{(-1)^{\nu+1}}{\alpha-\nu}$ und $\sum \frac{(-1)^{\nu+1}}{\beta-\nu}$ sind $O(1)$ nach dem Leibniz-Kriterium. Für $|\nu| > 4(\beta-\alpha)$ ist $\frac{1}{\alpha-\nu} < \frac{2}{\nu}$ sowie $\frac{1}{\beta-\nu} < \frac{2}{\nu}$, und daher

$$\left|\frac{1}{\alpha-\nu} - \frac{1}{\beta-\nu}\right| \;\le\; \frac{4(\beta-\alpha)}{\nu^2}\,.$$

Wir erhalten $\Sigma_1 \ll g(a) \cdot \log(\beta - \alpha + 2)$ und $\Sigma_2 \ll g(a)$. Damit ist

$$\sum_{\substack{\nu=-k \\ \nu \notin I}}^{k} J_1(\nu) \ \ll \ g(a) \cdot \log(\beta - \alpha + 2) \, . \tag{5}$$

Nach Lemma 1.6.1 ist

$$J_2(\nu) \ \ll \ |g'(a)| \cdot \left(\frac{1}{(\alpha - \nu)^2} + \frac{1}{(\beta - \nu)^2} \right) \tag{6}$$

und damit

$$\sum_{\substack{\nu=-k \\ \nu \notin I}}^{k} J_2(\nu) \ \ll \ |g'(a)| \, .$$

Aus (5) und (6) folgt

$$\sum_{\substack{\nu=-k \\ \nu \notin I}}^{k} \int_a^b g(t) e(f(t) - \nu t) dt \ \ll \ g(a) \cdot \log(\beta - \alpha + 2) + |g'(a)| \, ,$$

also

$$\sum_{\nu=-k}^{k} \int_a^b g(t) e(f(t) - \nu t) dt \ = \ \sum_{\alpha - \eta < \nu \leq \beta + \eta} \int_a^b g(t) e(f(t) - \nu t) dt \ + \ O\left(g(a) \cdot \log(\beta - \alpha + 2) \right) \ + \ O(|g'(a)|) \, .$$

Mit (3) folgt die Behauptung des Satzes. □

Satz 1.8.2
Es sei $a < b$, $f : [a, b] \to \mathbb{R}$ stetig differenzierbar und $f'(x)$ monoton. Es sei $|f'(x)| \leq \theta < 1$, dann gilt

$$\sum_{a < n \leq b} e(f(n)) \ = \ \int_a^b e(f(x)) dx \ + \ O_\theta(1) \, .$$

Beweis
Ohne Einschränkung können wir $f'(x)$ als monoton fallend annehmen. Wir wenden Satz 1.8.1 mit $\eta < 1 - \theta$ an, dann wird die Summationsbedingung $\alpha - \eta < \nu \leq \beta + \eta$ entweder allein für $\nu = 0$ oder für kein ν erfüllt. □

Satz 1.8.3 (Hardy-Littlewood-Approximation)
Es sei $\sigma \geq \sigma_0 > 0$ und $|t| < \frac{2\pi x}{C}$ für ein festes $C > 1$, dann gilt

$$\zeta(s) \ = \ \sum_{n \leq x} n^{-s} \ - \ \frac{x^{1-s}}{1-s} \ + \ O_{\sigma_0, C}(x^{-\sigma}) \, . \tag{HL}$$

Beweis
Nach der Eulerschen Summenformel gilt für $\sigma > 0$

$$\zeta(s) \ = \ \sum_{n=1}^{N} n^{-s} \ - \ s \int_N^\infty (u - [u] - \frac{1}{2}) u^{-s-1} du \ - \ \frac{N^{1-s}}{1-s} \ - \ \frac{1}{2} N^{-s} \tag{1}$$

(vgl. Übungsaufgaben 13 und 31 aus Funktionentheorie II). Wir wenden Satz 1.8.1 auf die Summe

$$\sum_{x < n \leq N} n^{-s}$$

an mit $f(u) = -\frac{t\log(u)}{2\pi}$ und $g(u) = u^{-s}$. Wegen der Bedingung $|t| < \frac{2\pi x}{C}$ gilt

$$\big|f'(u)\big| \;=\; \left|\frac{t}{2\pi u}\right| \;<\; 1$$

für $u > x$. Die Summationsbedingung $\alpha - \eta < \nu \le \beta + \eta$ ist für den einzigen Term $\nu = 0$ erfüllt, und wir erhalten

$$\sum_{x<n\le N} n^{-s} \;=\; \int_x^N u^{-s}du \;+\; O_{\sigma_0,C}(x^{-\sigma}) \;=\; -\frac{x^{1-s}}{1-s} \;+\; \frac{N^{1-s}}{1-s} \;+\; O_{\sigma_0,C}(x^{-\sigma})\,.$$

Die Behauptung (HL) folgt nun aus (1) für $N \to \infty$. □

Wählen wir x kleiner als durch die Bedingung $|t| < \frac{2\pi x}{C}$ vorgegeben, so wird die Bedingung $\alpha-\eta < \nu \le \beta+\eta$ noch von weiteren Werten außer für $\nu = 0$ erfüllt. Die daraus resultierenden Exponentialintegrale können asymptotisch ausgewertet werden. Dies soll im nächsten Lemma geschehen. Daraus werden wir dann eine schwache Form der approximativen Funktionalgleichung für die Riemannsche ζ-Funktion ableiten.

Lemma 1.8.4
Es sei $0 < \sigma < 1$, $x > 0$, $y = \frac{t}{2\pi x}$. *Für* $\nu < y - \eta$ *ist*

$$(1)\qquad \int_x^N e(\nu u)u^{-s}ds \;=\; \Gamma(1-s)\cdot\left(\frac{2\pi\nu}{i}\right)^{s-1} \;+\; O(N^{-\sigma}) \;+\; O\left(\frac{x^{1-\sigma}}{t}\right) \;+\; O\left(\frac{x^{1-\sigma}}{t}\cdot\frac{\nu}{\nu-y}\right)\,.$$

Für $y - \eta < \nu \le y + \eta$ *ist*

$$(2)\qquad \int_0^x u^{1-s}e(\nu u)du \;\ll\; x^{1-\sigma}\cdot\left(\frac{t}{y^2}\right)^{-\frac{1}{2}}\,.$$

Beweis
Wir zeigen zuerst

$$(3)\qquad \int_0^\infty e(\nu u)u^{-s}du \;=\; \Gamma(1-s)\cdot\left(\frac{2\pi\nu}{i}\right)^{s-1}\,.$$

Die Substitution $w = -2\pi i\nu u$ ergibt

$$\int_0^\infty e(\nu u)u^{-s}du \;=\; \left(\frac{2\pi\nu}{i}\right)^{s-1}\int_0^{-i\infty} w^{-s}e^{-w}dw\,.$$

Wir ersetzen nun den Integrationsweg $l_1 = [0, -i\infty)$ durch den Integrationsweg $[0, \infty)$. Dazu betrachten wir die geschlossene Kurve

$$S(\tau;\varepsilon,R) \;:=\; \begin{cases} \tau\varepsilon + (1-\tau)R & \text{falls}\quad 0 \le \tau \le 1 \\ \gamma(\tau;\varepsilon) & \text{falls}\quad 1 \le \tau \le 2 \\ -(3-\tau)i\varepsilon - (\tau-2)iR & \text{falls}\quad 2 \le \tau \le 3 \\ \varrho(\tau;R) & \text{falls}\quad 3 \le \tau \le 4 \end{cases}\,.$$

Dabei durchläuft $\gamma(\tau;\varepsilon)$ den Viertelkreis $\{|z| = \varepsilon\,,\ \mathrm{Re}(z) > 0\,,\ \mathrm{Im}(z) < 0\}$ im negativen Sinne, $\varrho(\tau;R)$ dagegen den Viertelkreis $\{|z| = R\,,\ \mathrm{Re}(z) > 0\,,\ \mathrm{Im}(z) < 0\}$ im positiven Sinne. Nach dem Cauchyschen Integralsatz ist

$$\int_{S(\ ;\varepsilon,R)} w^{-s}e^{-w}dw \;=\; 0\,.$$

Man zeigt leicht, dass

$$\lim_{\varepsilon\to 0+}\int\limits_{\gamma(\ ;\varepsilon)} w^{-s}e^{-w}dw \;=\; 0 \text{ sowie } \lim_{R\to\infty}\int\limits_{\varrho(\ ;R)} w^{-s}e^{-w}dw \;=\; 0$$

ist. Daher gilt

$$\int\limits_0^{-i\infty} w^{-s}e^{-w}dw \;=\; \int\limits_0^{\infty} w^{-s}e^{-w}dw \;=\; \Gamma(1-s)\,.$$

Damit ist (3) gezeigt. Partielle Integration ergibt

$$\int\limits_0^x e(\nu u)u^{-s}du \;=\; \left[\frac{u^{1-s}}{1-s}e(\nu u)\right]_0^x \;-\; \frac{2\pi i\nu}{1-s}\int\limits_0^x u^{1-s}e(\nu u)du\,. \tag{4}$$

Wir wenden Lemma 1.7.1 an mit $g(u)=u^{1-\sigma}$ und $f(u)=\nu u-\frac{t\log(u)}{2\pi}$. Dann ist

$$\frac{1}{f'(u)} \;=\; \frac{1}{\nu-\frac{t}{2\pi u}} \;<\; 0$$

und monoton fallend, also ist $-\frac{g(u)}{f'(u)}$ monoton wachsend. Lemma 1.7.1 ergibt

$$\int\limits_0^x u^{1-s}e(\nu u)du \;=\; O\left(\frac{x^{1-\sigma}}{\nu-y}\right)\,. \tag{5}$$

Aus (5) und (4) folgt

$$\int\limits_0^x u^{1-s}e(\nu u)du \;=\; O\left(\frac{x^{1-\sigma}}{t}\cdot\frac{\nu}{\nu-y}\right)\,. \tag{6}$$

Für hinreichend große N ist $\frac{u^{-\sigma}}{\nu-\frac{t}{2\pi u}}$ monoton fallend. Nach Lemma 1.7.1 erhalten wir

$$\int\limits_N^{\infty} e(\nu u)u^{-s}du \;\ll\; \frac{N^{-\sigma}}{\nu-\frac{t}{2\pi N}}\,. \tag{7}$$

Nach Lemma 1.7.2 folgt (2), und aus (3), (5), (6) und (7) folgt (1). □

Satz 1.8.5 (Approximative Funktionalgleichung, schwache Form)
Es sei $h>0$, $0<\sigma<1$ und $2\pi xy=t$ mit $x>h>0$, $y>h>0$. Dann gilt

$$\zeta(s) \;=\; \sum_{n\le x} n^{-s} \;+\; \chi(s)\sum_{n\le y} n^{s-1} \;+\; O_h(x^{-\sigma}\log|t|) \;+\; O_h(|t|^{\frac{1}{2}-\sigma}y^{\sigma-1}) \tag{1}$$

mit

$$\chi(s) \;=\; 2^{s-1}\cdot\pi^s\cdot\cos\left(\frac{\pi s}{2}\right)^{-1}\cdot\Gamma(s)^{-1} \;=\; 2^{s-1}\cdot\pi^s\cdot\frac{\sin(\pi s)}{\pi\cos(\frac{\pi s}{2})}\cdot\Gamma(1-s)\,.$$

Bemerkung 1.8.2
(1) hat starke formale Ähnlichkeit mit der exakten Funktionalgleichung

$$\zeta(s) \;=\; \chi(s)\zeta(1-s)$$

der Riemannschen ζ-Funktion, die auch - wie Satz 1.8.1 - mit der Poissonschen Summenformel bewiesen werden kann. Unter der approximativen Funktionalgleichung versteht man die Aussage

$$\zeta(s) \;=\; \sum_{n\le x} n^{-s} \;+\; \chi(s)\sum_{n\le y} n^{s-1} \;+\; O_h(x^{-\sigma}) \;+\; O_h(|t|^{\frac{1}{2}-\sigma}y^{\sigma-1})\,,$$

indem also das Restglied $O_h(x^{-\sigma}\log|t|)$ durch $O_h(x^{-\sigma})$ ersetzt ist. Für die meisten Anwendungen ist dieser Unterschied ohne Bedeutung.

Beweis von Satz 1.8.5
Wie im Beweis von Satz 1.8.3 gehen wir wieder von der Beziehung

$$\zeta(s) \;=\; \sum_{n=1}^{N} n^{-s} \;-\; \frac{N^{1-s}}{1-s} \;-\; s\int_{N}^{\infty}(u-[u]-\frac{1}{2})u^{-s-1}du \;-\; \frac{1}{2}N^{-s} \tag{2}$$

aus und wenden Satz 1.8.1 auf die Summe

$$\sum_{x<n\le N} n^{-s}$$

mit $f(u)=-\frac{t\log(u)}{2\pi}$ und $g(u)=u^{-\sigma}$ an. Also

$$\sum_{x<n\le N} n^{-s} \;=\; \sum_{-y-\eta<\nu\le-\frac{t}{2\pi N}+\eta}\int_{x}^{N} e(-\nu u)u^{-s}du \;+\; O\left(x^{-\sigma}\log(\tfrac{t}{x}-\tfrac{t}{N}+2)\right)\,.$$

Der Term für $\nu=0$ ergibt

$$\int_{x}^{N} u^{-s}du \;=\; -\frac{x^{1-s}}{1-s} \;+\; \frac{N^{1-s}}{1-s}\,.$$

Daher folgt mit (2):

$$\zeta(s) \;=\; \sum_{n\le x} n^{-s} \;+\; \sum_{1\le\nu\le y+\eta}\int_{x}^{N} e(\nu u)u^{-s}du \;+\; O_h\left(x^{-\sigma}\log(t)\right) \;+\; O_h(tN^{-\sigma})\,. \tag{3}$$

Mit Lemma 1.8.4 erhalten wir

$$\sum_{1\le\nu\le y+\eta}\int_{x}^{N} e(\nu u)u^{-s}du \;=\; \left(\frac{2\pi}{i}\right)^{s-1}\cdot\Gamma(1-s)\cdot\sum_{1\le\nu\le y-\eta}\nu^{s-1} \;+\; O\left(N^{-\sigma}\log(t)\right) \tag{4}$$

$$+\,O\left(\frac{x^{1-\sigma}}{t}\sum_{1\le\nu\le y-\eta}\frac{\nu}{\nu-y}\right) \;+\; O\left(x^{1-\sigma}\left(\tfrac{t}{x^2}\right)^{-\frac{1}{2}}\right)$$

$$=\; \left(\frac{2\pi}{i}\right)^{s-1}\cdot\Gamma(1-s)\cdot\sum_{1\le\nu\le y-\eta}\nu^{s-1} \;+\; O(N^{-\sigma}) \;+\; O\left(\frac{x^{1-\sigma}y\log(t)}{t}\right)\,.$$

Wegen

$$\chi(s) \;=\; 2^{s-1}\cdot\pi^{s}\cdot\frac{\sin(\pi s)}{\pi\cos(\frac{\pi s}{2})}\cdot\Gamma(1-s) \;=\; \frac{2^{s-1}}{i}\cdot\pi^{s-1}\cdot\left(e^{\frac{1}{2}\pi i s}-e^{-\frac{1}{2}\pi i s}\right)\cdot\Gamma(1-s)$$

$$=\; \left(\frac{2\pi}{i}\right)^{s-1}\cdot\Gamma(1-s)\cdot\left(1+O(e^{-\pi t})\right)$$

folgt die Behauptung aus (3) und (4) für $N\to\infty$. □

1.9. Abschätzung von Weylschen Exponentialsummen nach van der Corput

Die Ergebnisse des vorigen Abschnitts können auf die Abschätzung von Weylschen Exponentialsummen

$$\sum_{a<n\leq b} e(f(n))$$

selbst angewendet werden, wenn man über geeignete Schranken für die zweite Ableitung f'' verfügt.

Satz 1.9.1
Es sei $a < b$ mit $b \geq a+1$. Es sei $f : [a,b] \to \mathbb{R}$ zweimal stetig-differenzierbar und

$$0 \;<\; \lambda_2 \;\leq\; |f''(x)| \;\leq\; h \cdot \lambda_2 \,.$$

Dann ist

$$\sum_{a<n\leq b} e(f(n)) \;\ll\; h\cdot(b-a)\cdot\lambda_2^{\frac{1}{2}} \;+\; \lambda_2^{-\frac{1}{2}} \,.$$

Beweis
Wir können $\lambda_2 < 1$ annehmen, da die Behauptung sonst trivial ist. Die Voraussetzungen von Satz 1.8.1 sind dann erfüllt. Es sei $f'(b) = \alpha$ sowie $f'(a) = \beta$. Nach Satz 1.8.1 ist mit beliebigem η und $0 < \eta < 1$ dann

$$\sum_{a<n\leq b} e(f(n)) \;=\; \sum_{a-\eta<\nu\leq\beta+\eta} \int_a^b e(f(x)-\nu x)dx \;+\; O(\log(\beta-\alpha+2)) \,.$$

Nach Lemma 1.7.2 ist

$$\int_a^b e(f(x)-\nu x)dx \;\ll\; \lambda_2^{-\frac{1}{2}} \tag{1}$$

für alle ν. Es ist

$$\beta-\alpha \;=\; f'(b)-f'(a) \;=\; O\left((b-a)\cdot h\cdot\lambda_2\right) \,, \tag{2}$$

und wegen

$$\log(\beta-\alpha+2) \;=\; O(\log(\beta-\alpha+2)) \;=\; O((b-a)\lambda_2) \;+\; O(1) \;=\; O((b-a)\cdot h\cdot\lambda_2^{\frac{1}{2}}) \;+\; O(1) \,.$$

folgt die Behauptung. □

Exponentialsummen können auch behandelt werden, indem man zuerst einen - oder mehrere - verallgemeinerte Weylschritte anwendet, und den van der Corput-Schritt (Satz 1.8.1) auf die daraus entstehenden neuen Exponentialsummen. Man kann die Schritte auch beliebig hintereinander schalten.

Satz 1.9.2 (Weylschritt)
Es sei $f : [a,b] \to \mathbb{R}$, $a < u \leq b$, $1 \leq q \leq b-a$, dann ist

$$\left|\sum_{a<n\leq b} e(f(n))\right| \;\ll\; \frac{b-a}{q^{\frac{1}{2}}} \;+\; \left(\frac{b-a}{q}\sum_{\nu=1}^{q-1}\left|\sum_{a<n\leq b-\nu} e(f(n+\nu)-f(n))\right|\right)^{\frac{1}{2}} \,.$$

Beweis
Wir definieren $e(f(n)) = 0$ falls $n \leq a$ oder $n > b$ ist. Es ist

$$\sum_{a<n\leq b} e(f(n)) \;=\; \frac{1}{q}\sum_{a<n\leq b}\sum_{\nu=1}^{q} e(f(n+\nu)) \;+\; \theta(q+1)$$

mit $|\theta| \le 1$ (vgl. Übungsaufgabe 9). Anwendung der Cauchy-Schwarzschen Ungleichung ergibt

$$\left|\sum_{a<n\le b} e(f(n))\right|^2 \ll \frac{1}{q^2}\cdot(b-a)\cdot\sum_{a<n\le b}\left|\sum_{\nu=1}^{q} e(f(n+\nu))\right|^2 . \tag{1}$$

Es ist

$$\sum_{a<n\le b}\left|\sum_{\nu=1}^{q} e(f(n+\nu))\right|^2 = \sum_{\nu_1=1}^{q}\sum_{\nu_2=1}^{q}\sum_{a<n\le b} e(f(n+\nu_2)-f(n+\nu_1)) = \Sigma_1 + 2\Sigma_2$$

mit

$$\Sigma_1 = \sum_{\substack{1\le\nu_1,\nu_2\le q\\ \nu_1=\nu_2}}\sum_{a<n\le b} e(f(n+\nu_2)-f(n+\nu_1)) \ , \ \Sigma_2 = \sum_{\substack{1\le\nu_1,\nu_2\le q\\ \nu_1<\nu_2}}\sum_{a<n\le b} e(f(n+\nu_2)-f(n+\nu_1)) .$$

Wir haben

$$\Sigma_1 \ll q(b-a) . \tag{2}$$

Für ein festes Paar (m,ν) mit $1 \le \nu \le q-1$ und $m \in \mathbb{Z}$ gibt es $(q-\nu)$ Tripel (n,ν_1,ν_2) mit $1 \le \nu_1 \le q$, $1 \le \nu_2 \le q$ und $n+\nu_1 = m$, $n+\nu_2 = m+\nu$. Also

$$\Sigma_2 = \sum_{\nu=1}^{q-1}(q-\nu)\sum_{m} e(f(m+\nu)-f(m)) \le q\sum_{\nu=1}^{q-1}\left|\sum_{m} e(f(m+\nu)-f(m))\right| . \tag{3}$$

Aus (1), (2) und (3) folgt die Behauptung. □

So wie in der Weylschen Methode die Polynome k-ten Grades P_k im Weylschritt durch die Anwendung der Differenzenoperatoren Δ_ν durch Polynome $(k-1)$-ten Grades $\Delta_\nu(P_k)$ ersetzt werden, so können jetzt Funktionen f, für deren k-te Ableitung Schranken gegeben sind, durch Funktionen $\Delta_\nu(f)$ ersetzt werden, für deren $(k-1)$-te Ableitung Schranken vorliegen.

Satz 1.9.3
Es sei $a < n \le b$ mit $b-a \ge 1$. Es sei $f : [a,b] \to \mathbb{R}$ dreimal stetig-differenzierbar und

$$\lambda_3 \le |f'''(x)| \le h\cdot\lambda_3 ,$$

dann ist

$$\sum_{a<n\le b} e(f(n)) \ll h^{\frac12}\cdot(b-a)\cdot\lambda_3^{\frac16} + (b-a)^{\frac12}\lambda_3^{-\frac16} .$$

Beweis
Wir können $\lambda_3 \le 1$ und $\lambda_3^{-\frac13} \le b-a$ voraussetzen, da sonst die Behauptung trivial ist. Es sei

$$g(x) = \Delta_\nu(f)(x) = f(x+\nu)-f(x) ,$$

dann ist

$$g''(x) = f''(x+\nu)-f''(x) = \nu\cdot f'''(x+\theta\nu) \tag{1}$$

mit $0 < \theta < 1$ nach dem Mittelwertsatz. Nach dem Weylschritt 1.9.2 haben wir

$$\sum_{a<n\le b} e(f(n)) \ll \frac{b-a}{q^{\frac12}} + \left(\frac{b-a}{q}\sum_{\nu=1}^{q-1}\left|\sum_{a<n\le b-\nu}\Delta_\nu(f)(n)\right|\right)^{\frac12} .$$

Mit Satz 1.9.1 und (1) folgt

$$\sum_{a<n\le b} e(f(n)) \ll \frac{b-a}{q^{\frac12}} + \left(\frac{b-a}{q}\sum_{\nu=1}^{q-1}\left(h(b-a)\nu^{\frac12}\lambda_3^{\frac12} + \nu^{-\frac12}\lambda_3^{-\frac12}\right)\right)^{\frac12}$$

$$\ll \frac{b-a}{q^{\frac{1}{2}}} + \left(h(b-a)^2 q^{\frac{1}{2}} \lambda_3^{\frac{1}{2}} + (b-a) q^{-\frac{1}{2}} \lambda_3^{-\frac{1}{2}}\right)^{\frac{1}{2}}$$

$$\ll (b-a) q^{-\frac{1}{2}} + h^{\frac{1}{2}} (b-a) q^{\frac{1}{4}} \lambda_3^{\frac{1}{4}} + (b-a)^{\frac{1}{2}} q^{-\frac{1}{4}} \lambda_3^{-\frac{1}{4}} .$$

Die beiden ersten Terme sind von der selben Größenordnung (in λ_3), wenn $q = [\lambda_3^{-\frac{1}{3}}]$ ist. Daraus folgt die Behauptung. □

Wir behandeln nun den allgemeinen Fall, in dem Schranken für die k-te Ableitung existieren. Im Hinblick auf Anwendungen ist es wichtig, dass die in den O- und $\ll$-Abschätzungen impliziten Konstanten unabhängig von k gewählt werden können.

Satz 1.9.4
Es sei $k \geq 3$, $f : [a,b] \to \mathbb{R}$ k-mal stetig-differenzierbar, sowie

$$\lambda_k \leq |f^{(k)}(x)| \leq h \cdot \lambda_k \ , \ b-a \geq 1 \ , \ K = 2^{k-1} ,$$

dann ist

$$\sum_{a<n\leq b} e(f(n)) \ll h^{\frac{2}{K}} (b-a) \lambda_k^{\frac{1}{(2K-2)}} + (b-a)^{1-\frac{2}{K}} \lambda_k^{-\frac{1}{2K-2}} .$$

Beweis
Wir können wieder $\lambda_k < 1$ und $f^{(k)}(x) > 0$ annehmen. Außerdem können wir

$$2\lambda_k^{-\frac{1}{K-1}} \leq b-a \tag{1}$$

annehmen, da sonst $\lambda_k^{-\frac{1}{2K-2}} \geq \frac{1}{2}(b-a)^{\frac{1}{2}}$, also $(b-a)^{1-\frac{1}{2K}} \lambda_k^{-\frac{1}{2K-2}} \geq \frac{1}{2}(b-a)$ ist. Wir führen den Beweis durch Induktion nach k. Der Fall $k=3$ ist Satz 1.9.3, es bleibt also noch der Schritt $k-1 \to k$ zu zeigen. Dazu sei $g(x) = f(x+\nu) - f(x)$, dann ist

$$g^{(k-1)}(x) = f^{(k-1)}(x+\nu) - f^{(k-1)}(x) = \nu \cdot f^{(k)}(\xi)$$

mit $x < \xi < x+\nu$ nach dem Mittelwertsatz. Deshalb gilt

$$\nu\lambda_k \leq g^{(k-1)}(x) \leq h\nu\lambda_k .$$

Nach Induktionsannahme folgt

$$\left| \sum_{a<n\leq b} e(g(n)) \right| < A_1 h^{\frac{4}{K}} (b-a) (\nu\lambda_k)^{\frac{1}{K-2}} + A_2 (b-a)^{1-\frac{4}{K}} \cdot (\nu\lambda_k)^{-\frac{1}{K-2}}$$

mit absoluten Konstanten $A_1, A_2 > 0$. Deshalb gilt für $1 \leq q \leq b-a$:

$$\sum_{\nu=1}^{q-1} \left| \sum_{a<n\leq b-\nu} e(g(n)) \right| < A_1 h^{\frac{4}{K}} (b-a) q^{1+\frac{1}{K-2}} \lambda_k^{\frac{1}{K-2}} + 2A_2 (b-a)^{1-\frac{4}{K}} q^{1-\frac{1}{K-2}} \lambda_k^{-\frac{1}{K-2}} , \tag{2}$$

da wegen $k \geq 4$

$$\sum_{\nu=1}^{q-1} \nu^{-\frac{1}{K-2}} < \int_0^q u^{-\frac{1}{K-2}} du = \frac{q^{1-\frac{1}{K-2}}}{1-\frac{1}{K-2}} \leq 2q^{1-\frac{1}{K-2}}$$

gilt. Nach dem Weylschritt 1.9.2 und (2) folgt mit absoluten Konstanten $A_3, A_4 > 0$:

$$\sum_{a<n\leq b} e(f(n))$$

$$\leq\ A_3(b-a)q^{-\frac{1}{2}}\ +\ A_4(b-a)^{\frac{1}{2}}q^{-\frac{1}{2}}\cdot\left(A_1h^{\frac{4}{K}}(b-a)q^{1+\frac{1}{K-2}}\lambda_k^{-\frac{1}{K-2}}+2A_2(b-a)^{1-\frac{4}{K}}q^{1-\frac{1}{K-2}}\lambda_k^{-\frac{1}{K-2}}\right)^{\frac{1}{2}}$$

$$\leq\ A_3(b-a)q^{-\frac{1}{2}}\ +\ A_4A_1^{\frac{1}{2}}h^{\frac{2}{K}}(b-a)q^{\frac{1}{2K-4}}\lambda_k^{\frac{1}{2K-4}}\ +\ A_4(2A_2)^{\frac{1}{2}}(b-a)^{1-\frac{2}{K}}q^{-\frac{1}{2K-4}}\lambda_k^{-\frac{1}{2K-4}}\ .$$

Wir wählen nun $q=q(\lambda_k)$ so, dass in den ersten beiden Termen die gleiche Potenz von λ_k auftritt, d. h. $q=[\lambda_k^{-\frac{1}{K-1}}]+1$. Die Bedingung $q\leq b-a$ in Satz 1.9.2 ist wegen (1) erfüllt. Es ist

$$\lambda_k^{-\frac{1}{K-1}}\ \leq\ q\ \leq\ 2\lambda_k^{-\frac{1}{K-1}}\ ,\ \ q^{\frac{1}{2K-4}}\lambda_k^{\frac{1}{2K-4}}\ \leq\ 2^{\frac{1}{2K-4}}\lambda_k^{\frac{1}{2K-4}(1-\frac{1}{K-1})}\ \leq\ 2\lambda_k^{\frac{1}{2K-2}}\ ,$$

und wir erhalten

$$\left|\sum_{a<n\leq b}e(f(n))\right|\ \leq\ \left(A_3+2A_4A_1^{\frac{1}{2}}\right)h^{\frac{2}{K}}(b-a)\lambda_k^{\frac{1}{2K-2}}\ +\ A_4(2A_2)^{\frac{1}{2}}(b-a)^{1-\frac{2}{K}}\lambda_k^{-\frac{1}{2K-2}}\ .$$

Bis auf die Konstanten ist dies die Behauptung für k. Wenn A_1 und A_2 hinreichend groß sind, ist

$$A_3+2A_4A_1^{\frac{1}{2}}\ \leq\ A_1\ ,\ \ A_4(2A_2)^{\frac{1}{2}}\ \leq\ A_2\ ,$$

womit der Induktionsschluss $k-1\to k$ durchgeführt ist. □

1.10. Größenordnung der Riemannschen ζ-Funktion im kritischen Streifen

Satz 1.10.1
Es sei $l\geq 3$ und $L=2^{l-1}$, für $\sigma=1-\frac{l}{2L-2}$ gilt dann

$$\zeta(\sigma+it)\ \ll\ t^{\frac{1}{2L-2}}\cdot\log|t|\ ,$$

wobei die O-Konstante von l unabhängig ist.

Beweis
Es genügt, den Beweis für $t\geq 0$ zu führen. Wir gehen von der Hardy-Littlewood-Abschätzung (Satz 1.8.3)

$$\zeta(s)\ =\ \sum_{n\leq x}n^{-s}\ -\ \frac{x^{1-s}}{1-s}\ +\ O_{\sigma,C}\left(x^{-\sigma}\right)\tag{1}$$

aus für $\sigma=\sigma_0>0$, $t<\frac{2\pi x}{C}$, und können $\sigma_0\geq\frac{1}{2}$ annehmen. Wir wenden Satz 1.9.4 an mit

$$f(x)\ =\ -\frac{t\cdot\log(x)}{2\pi}\ ,\ \ f^{(k)}(x)\ =\ \frac{(-1)^k(k-1)!\cdot t}{2\pi x^k}\ .$$

Für $a<n\leq b\leq 2a$ ist

$$\frac{(k-1)!\cdot t}{2\pi(2a)^k}\ \leq\ \left|f^{(k)}(n)\right|\ \leq\ \frac{(k-1)!\cdot t}{2\pi a^k}\ .$$

Die Voraussetzungen von Satz 1.9.4

$$\lambda_k\ \leq\ \left|f^{(k)}(x)\right|\ \leq\ h\cdot\lambda_k$$

sind also erfüllt mit der Wahl

$$\lambda_k\ =\ \frac{(k-1)!\cdot t}{2\pi(2a)^k}\ \ ,\ \ \ h\ =\ 2^k\ .$$

Wir erhalten

$$\sum_{a<n\leq b}n^{-it}\ \ll\ 2^{\frac{2k}{K}}\cdot a\cdot\left(\frac{(k-1)!\cdot t}{2\pi(2a)^k}\right)^{\frac{1}{2K-2}}\ +\ a^{1-\frac{2}{K}}\cdot\left(\frac{(k-1)!\cdot t}{2\pi(2a)^k}\right)^{-\frac{1}{2K-2}}$$

$$\ll a^{1-\frac{k}{2K-2}} \cdot t^{\frac{1}{2K-2}} + a^{1-\frac{2}{K}+\frac{k}{2K-2}} \cdot t^{-\frac{1}{2K-2}} .$$

Die beiden Terme sind gleich, falls $a = t^{\frac{K}{kK-2K+2}}$ ist. Falls daher

$$a \ < \ A \cdot t^{\frac{K}{kK-2K+2}} \tag{2}$$

mit einer absoluten Konstanten $A > 0$ gilt, kann der zweite Term weggelassen werden. Gilt (2), so folgt durch partielle Summation

$$\sum_{a<n\leq b} n^{-s} \ \ll \ a^{1-\sigma-\frac{k}{2K-2}} \cdot t^{\frac{1}{2K-2}}$$

und mit $\sigma = 1 - \frac{l}{2L-2}$ dann

$$\sum_{a<n\leq b} n^{-s} \ \ll \ a^{\frac{l}{2L-2}-\frac{k}{2K-2}} \cdot t^{\frac{1}{2K-2}} . \tag{3}$$

Wir wenden dies mit $k := l$ an und erhalten

$$\sum_{a<n\leq b} n^{-s} \ \ll \ t^{\frac{1}{2L-2}} \tag{4}$$

für $a < A \cdot t^{\frac{L}{lL-2L+2}}$. Daraus folgt

$$\sum_{n\leq t^{\frac{L}{lL-2L+2}}} \ = \ \sum_j \sum_n n^{-s} ,$$

wobei über die (j, n) summiert wird mit

$$1 \ \leq \ 2^j \ \leq \ t^{\frac{L}{lL-2L-1}} \quad , \quad 2^{-j-1} \cdot t^{\frac{L}{lL-2L+2}} \ < \ n \ \leq 2^{-j} \cdot t^{\frac{L}{lL-2L+2}} .$$

Da über $O(\log(t))$ Werte von j summiert wird ist wegen (4)

$$\sum_{n\leq t^{\frac{L}{lL-2L+2}}} n^{-s} \ \ll \ t^{\frac{1}{2L-2}} \cdot \log(t) . \tag{5}$$

Wir behandeln nun die Summe

$$\sum_{t^{\frac{L}{lL-2L+2}}<n\leq t} \ = \ \sum_j \sum_{2^{-j}t<n\leq 2^{1-j}t} ,$$

wobei über alle j summiert wird mit

$$t^{\frac{L}{lL-2L+2}} \ \leq \ 2^{-j}t \ \leq \ t .$$

Zu jedem j gibt es ein $k < l$, so dass

$$t^{\frac{K}{(k+1)K-2K+1}} \ < \ 2^{-j}t \ \leq \ t^{\frac{K}{kK-2K+2}} .$$

Dann ist nach (3)

$$\sum_{2^{-j}t<n\leq 2^{1-j}t} n^{-s} \ \ll \ \exp\left(\log(t) \cdot \left(\left(\frac{l}{2L-2} - \frac{k}{2K-2}\right) \cdot \frac{K}{(k+1)K-2K+1} + \frac{1}{2K-2}\right)\right) . \tag{6}$$

Nun ist $2^{l-k} \geq l-k$ und daher $(L-K) \geq (l-k)K$. Daraus folgt weiter $(K-1)(L-K) \geq (K-1)(l-k)$ und

$$-k(L-K)K - (L-K)K + (K-L)(1-2K) \ \geq \ ((l-k)K - k(L-K) + (k-l)K)$$

und schließlich

$$\left(\frac{l}{2L-2} - \frac{k}{2K-2}\right) \cdot \frac{K}{(k+1)K-2K+1} + \frac{1}{2K-2} \ \leq \ \frac{1}{2L-2} . \tag{7}$$

Aus (5), (6) und (7) folgt die Behauptung. □

Im Hinblick auf weitere Anwendungen formulieren wir nun einen allgemeinen Zusammenhang zwischen der Größenordnung der Riemannschen ζ-Funktion in der Nähe von $\sigma = 1$, sowie der Weite der nullstellenfreien Zone von $\zeta(s)$, die wiederum Konsequenzen für die Verteilung der Primzahlen hat. Zur Vorbereitung beweisen wir zwei funktionentheoretische Lemmata:

Lemma 1.10.2
Es sei f holomorph und $M > 1$, so dass

$$\left|\frac{f(s)}{f(s_0)}\right| \;<\; e^M$$

auf der Kreisscheibe $|s - s_0| < r$ gilt. Dann ist mit einer absoluten Konstante $A > 0$

$$\left|\frac{f'(s)}{f(s)} - \sum_{\varrho}\frac{1}{s-\varrho}\right| \;<\; \frac{AM}{r} \quad \textit{für} \quad |s - s_0| \;\leq\; \tfrac{1}{4}r\,,$$

wobei ϱ alle Nullstellen von f mit $|\varrho - s_0| \leq \frac{1}{2}r$ durchläuft.

Beweis
Die Funktion

$$g(s) \;=\; f(s)\cdot\prod_{\varrho}(s-\varrho)^{-1}$$

ist für $|s - s_0| < r$ holomorph und auf der kleineren Kreisscheibe $|s - s_0| \leq \frac{1}{2}r$ von Null verschieden. Auf dem Rand $|s - s_0| = r$ gilt

$$|s-\varrho| \;\geq\; \tfrac{1}{2}r \;\geq\; |s_0-\varrho|\,,$$

und damit

$$\left|\frac{g(s)}{g(s_0)}\right| \;=\; \left|\frac{f(s)}{f(s_0)}\right|\cdot\left|\prod_{\varrho}\frac{s_0-\varrho}{s-\varrho}\right| \;\leq\; \left|\frac{f(s)}{f(s_0)}\right| \;<\; e^M\,.$$

Nach dem Maximumsprinzip gilt diese Ungleichung dann auch auf der Kreisscheibe $|s - s_0| \leq r$. Wir setzen

$$h(s) \;=\; \mathrm{Log}\left(\tfrac{g(s)}{g(s_0)}\right)\,,$$

dann ist $h(s)$ holomorph für $|s - s_0| \leq \frac{1}{2}r$. Zudem ist $h(s_0) = 0$ und $\mathrm{Re}(h(s)) \leq M$, nach dem Satz von Borel-Carathéodory (Lemma 7.3.8 aus Funktionentheorie II) gibt es eine absolute Konstante $A_1 > 0$, so dass $|f(s)| < A_1 M$ ist für $|s - s_0| \leq \frac{3}{8}r$. Nach der Cauchyschen Integralformel gilt für $|s - s_0| \leq \frac{1}{4}r$ dann

$$|h'(s)| \;=\; \left|\frac{1}{2\pi i}\int\limits_{|z-s|=\frac{3}{8}r}\frac{h(z)}{(z-s)^2}dz\right| \;<\; \frac{A_2 M}{r}$$

mit einer absoluten Konstante $A_2 > 0$. □

Lemma 1.10.3
Es sei f holomorph und $M > 1$ mit

$$\left|\frac{f(s)}{f(s_0)}\right| \;<\; e^M$$

für $|s - s_0| < r$, und f habe zusätzlich keine Nullstellen im Halbkreis $\{|s - s_0| \leq r\,,\, \mathrm{Re}(s) > \mathrm{Re}(s_0)\}$. Dann gilt

(i)
$$-\mathrm{Re}\left(\tfrac{f'(s_0)}{f(s_0)}\right) \;<\; \frac{AM}{r}\,.$$

Hat f eine Nullstelle ϱ_0 auf der Strecke zwischen $s_0 - \frac{1}{2}r$ und s_0, so gilt

(ii) $$-\mathrm{Re}\left(\frac{f'(s_0)}{f(s_0)}\right) \;<\; \frac{AM}{r} - \frac{1}{s_0 - \varrho_0}\,.$$

$A > 0$ ist jeweils eine absolute Konstante.

Beweis
Nach Lemma 1.10.2 gilt

$$-\mathrm{Re}\left(\frac{f'(s_0)}{f(s_0)}\right) \;<\; \frac{AM}{r} \;-\; \sum_{|\varrho - s_0| \le \frac{1}{2}r} \mathrm{Re}\left(\tfrac{1}{s_0-\varrho}\right)\,.$$

Aus $\mathrm{Re}(\frac{1}{s_0-\varrho}) \ge 0$ für alle ϱ folgt die Behauptung. □

Satz 1.10.4
Es sei $\zeta(s) \ll e^{\Phi(t)}$ für $t \to \infty$ in dem Gebiet $1 - \theta(t) \le \sigma \le 2$ (und $t \ge 0$), wobei $\Phi(t)$ und $\frac{1}{\theta(t)}$ positiv und monoton wachsend in t sind für $t \ge 0$, sowie

$$\theta(t) \;\le\; 1 \;\;,\;\; \Phi(t) \;\longrightarrow\; \infty \;\;,\;\; \frac{\Phi(t)}{\theta(t)} e^{-\Phi(t)} \;\longrightarrow\; 0 \;\; \textit{für } t \to \infty\,.$$

Dann gibt es eine Konstante $A_1 > 0$, so dass $\zeta(s)$ keine Nullstellen im Gebiet

$$\left\{\sigma \;\ge\; 1 - A_1 \frac{\theta(2t+1)}{\Phi(2t+1)}\right\}$$

besitzt.

Beweis
Es sei $\beta + \gamma i$ eine Nullstelle von $\zeta(s)$ in der oberen Halbebene. Die Konstanten $A_k > 0$ für $k \ge 2$ werden im Folgenden höchstens von den Funktionen θ und Φ abhängen. Es sei σ_0 beliebig mit

(1) $$1 + e^{-\Phi(2\gamma+1)} \;\le\; \sigma_0 \;\le 2\,,$$

sowie

(2) $$s_0 \;=\; \sigma_0 + i\gamma\,,\; s_0' \;=\; \sigma_0 + 2i\gamma\,,$$

(3) $$r \;=\; \theta(2\gamma+1)\,.$$

Da $\theta(t)$ monoton fällt, liegen die Kreisscheiben $|s - s_0| \le r$, $|s - s_0'| \le r$ beide im Bereich $\{\sigma + it \mid \sigma \ge 1 - \theta(t)\}$. Wegen $|\zeta(s_0)|^{-1} < \exp(A \cdot \Phi(2\gamma+1))$ bzw. $|\zeta(s_0')|^{-1} < \exp(A \cdot \Phi(2\gamma+1))$ für genügend großes A existiert eine Konstante $A_2 > 0$, so dass

(4) $$\left|\frac{\zeta(s)}{\zeta(s_0)}\right| \;<\; e^{A_2\Phi(2\gamma+1)} \;\text{ bzw. }\; \left|\frac{\zeta(s)}{\zeta(s_0')}\right| \;<\; e^{A_2\Phi(2\gamma+1)}$$

gilt auf den Kreisscheiben $|s - s_0| \le r$ bzw. $|s - s_0'| \le r$. Wir wenden jetzt Lemma 1.10.3 an mit $M = A_2\Phi(2\gamma+1)$ und erhalten

(5) $$-\mathrm{Re}\left(\tfrac{\zeta'(\sigma_0+2i\gamma)}{\zeta(\sigma_0+2i\gamma)}\right) \;<\; A_3 \frac{\Phi(2\gamma+1)}{\theta(2\gamma+1)}\,.$$

Wir behandeln zunächst

Fall I: Es gelte

(6) $$\beta \;>\; \sigma_0 - \tfrac{1}{2}r\,.$$

Wir erhalten wegen 1.10.3(ii) in diesem Fall

(7) $$-\mathrm{Re}\left(\tfrac{\zeta'(\sigma_0+i\gamma)}{\zeta(\sigma_0+i\gamma)}\right) \;<\; A_3 \frac{\Phi(2\gamma+1)}{\theta(2\gamma+1)} - \frac{1}{\sigma_0 - \beta}\,.$$

Es ist

$$-\frac{\zeta'(\sigma_0)}{\zeta(\sigma_0)} \;<\; \frac{a}{\sigma_0-1} \;\text{ mit } a \;=\; a(\sigma_0) \;\longrightarrow\; 1 \;\text{ für }\; \sigma_0 \to 1\,. \tag{8}$$

Wie im Beweis für $\zeta(1+it) \neq 0$ von Hadamard und de la Vallée-Poussin verwenden wir nun die Ungleichung

$$-3\frac{\zeta'(\sigma_0)}{\zeta(\sigma_0)} - 4\mathrm{Re}\left(\tfrac{\zeta'(\sigma_0+i\gamma)}{\zeta(\sigma_0+i\gamma)}\right) - \mathrm{Re}\left(\tfrac{\zeta'(\sigma_0+2i\gamma)}{\zeta(\sigma_0+2i\gamma)}\right) \;\geq\; 0 \tag{9}$$

für $\sigma > 1$. Wir wenden (9) an mit $\sigma = \sigma_0$ und erhalten mit (5), (7) und (8) dann

$$\frac{3a}{\sigma_0-1} + \frac{5A_3\Phi(2\gamma+1)}{\theta(2\gamma+1)} - \frac{4}{\sigma_0-\beta} \;\geq\; 0\,,$$

also

$$\sigma_0 - \beta \;\geq\; \left(\frac{3a}{4(\sigma_0-1)} + \frac{5A_3}{4}\cdot\frac{\Phi(2\gamma+1)}{\theta(2\gamma+1)}\right)^{-1}\,,$$

und somit

$$1-\beta \;\geq\; \left(\frac{3a}{4(\sigma_0-1)} + \frac{5A_3}{4}\cdot\frac{\Phi(2\gamma+1)}{\theta(2\gamma+1)}\right)^{-1} - (\sigma_0-1) \;=\; \frac{1-\frac{3}{4}a-\frac{5}{4}A_3\cdot\frac{\Phi(2\gamma+1)\cdot(\sigma_0-1)}{\theta(2\gamma+1)}}{\frac{3a}{4(\sigma_0-1)}+\frac{5}{4}A_3\cdot\frac{\Phi(2\gamma+1)}{\theta(2\gamma+1)}}\,. \tag{10}$$

Für hinreichend große γ können wir wegen (1)

$$\sigma_0 - 1 \;=\; \frac{1}{40A_3}\cdot\frac{\theta(2\gamma+1)}{\Phi(2\gamma+1)} \tag{11}$$

und wegen (8) $a = \frac{5}{4}$ wählen. Wir erhalten aus (10)

$$1-\beta \;\geq\; \frac{\theta(2\gamma+1)}{1240A_3\Phi(2\gamma+1)}$$

und damit die Behauptung des Satzes.

Fall II:
Es gelte

$$\beta \;\leq\; \sigma_0 - \tfrac{1}{2}r \;=\; 1 + \frac{1}{40A_3}\cdot\frac{\theta(2\gamma+1)}{\Phi(2\gamma+1)} - \tfrac{1}{2}\theta(2\gamma+1)\,. \tag{12}$$

Dies ergibt ebenfalls die Behauptung. □

Korollar 1.10.5
Es gibt eine absolute Konstante $A_0 > 0$, so dass $\zeta(s) \neq 0$ für $t \geq 0$ und $\sigma \geq 1 - \frac{A_0}{\log(t)}$ ist.

Beweis
Nach der Hardy-Littlewood-Approximation 1.8.3 folgt, dass $|\zeta(\sigma+it)| \ll t^{\frac{1}{2}}$ ist für $\sigma \geq \frac{1}{2}$ und $t \geq 1$. Wir wenden Satz 1.10.4 an mit $\theta(t) = \frac{1}{2}$ und $\Phi(t) = \log(t)$, und erhalten $\zeta(s) \neq 0$ für

$$\sigma \;\geq\; 1 - A_1\frac{\theta(2t+1)}{\Phi(2t+1)} \;\geq\; 1 - \frac{A_0}{\log(t)}\,.$$

□

Mittels der Abschätzungen von Satz 1.10.1, also mittels Weylscher Exponentialsummen, lässt sich dieses Ergebnis leicht verbessern.

Satz 1.10.6 (Nullstellenfreie Zone der ζ-Funktion)
Es gibt eine absolute Konstante $A_0 > 0$, so dass $\zeta(s) \neq 0$ ist für $t \geq 0$ und

$$\sigma \ \geq \ 1 - A_0 \frac{\log(\log(t))}{\log(t)} \, .$$

Beweis
Nach Satz 1.10.1 ist

$$\zeta(s) \ \ll \ t^{\frac{1}{2L-2}} \cdot \log(t) \tag{1}$$

für $\sigma = 1 - \frac{l}{2L-2}$ und $l \geq 3$. Es sei $t \geq t_0$ gegeben. Die folgende Definition und die Abschätzungen gelten für hinreichend großes t_0. Wir setzen

$$l \ = \ \left[\frac{1}{\log(2)} \cdot \log \left(\frac{\log(t)}{\log(\log(t))} \right) \right]$$

und nehmen $l \geq 3$ an. Dann ist

$$L \ \leq \ 2^{\frac{1}{\log(2)} \log\left(\frac{\log(t)}{\log(\log(t))} \right) - 1} \ = \ \frac{1}{2} \cdot \frac{\log(t)}{\log(\log(t))} \, ,$$

sowie

$$L \ \geq \ \frac{1}{4} \cdot \frac{\log(t)}{\log(\log(t))} \, .$$

Deshalb

$$\frac{l}{2L-2} \ \geq \ \frac{l}{2L} \ \geq \ \frac{\log(\log(t)) - \log(\log(\log(t))) - \log(2)}{\log(2)} \cdot \frac{\log(\log(t))}{\log(t)} \ \geq \ \frac{(\log(\log(t)))^2}{\log(t)} \, .$$

Deshalb ist $\sigma \geq 1 - \frac{l}{2L-2}$, falls $\sigma \geq 1 - \frac{(\log(\log(t))^2}{\log(t)}$ ist. Nach (1) folgt

$$\zeta(s) \ \ll \ t^{\frac{1}{2L-2}} \cdot \log(t) \ \ll \ t^{\frac{1}{L}} \cdot \log(t) \ \ll \ t^{\frac{4 \log(\log(t))}{\log(t)}} \cdot \log(t) \ = \ \log(t)^5 \, .$$

Wir wenden jetzt Satz 1.10.4 an mit

$$\theta(t) \ = \ \frac{(\log(\log(t)))^2}{\log(t)} \ , \ \ \Phi(t) \ = \ 5 \log(\log(t))$$

und erhalten die Behauptung. □

1.11. Mittelwertsatz für Dirichletpolynome und die Riemannsche ζ-Funktion

Satz 1.11.1
Es sei

$$S(s) \ = \ \sum_{n=1}^{N} a_n n^{-s} \, , \ a_n \in \mathbb{C} \, , \ T > 0 \, .$$

Dann gilt

$$\int_{T_0}^{T_0+T} |S(it)|^2 dt \ = \ (T + O(N \log(N))) \cdot \left(\sum_{n=1}^{N} |a_n|^2 \right) \, .$$

Beweis
Der Beweis ähnelt dem Beweis der Parsevalschen Gleichung (vgl. Übungsaufgabe 8). Während dort die Funktionen

$$e_{q,m} : \ n \longmapsto e(\tfrac{mn}{q})$$

strikt orthogonal sind, d. h.

$$\langle e_{q,m_1}|e_{q,m_2}\rangle \;=\; \frac{1}{q}\sum_{n=0}^{q-1} e\left(\tfrac{(m_1-m_2)n}{q}\right) \;=\; \begin{cases}1 & \text{falls} \quad m_1=m_2\\ 0 & \text{falls} \quad m_1\neq m_2\end{cases},$$

sind die entsprechenden Funktionen $f_n:\; t\longmapsto n^{-it}$ im jetzigen Fall nur annähernd orthogonal bzgl. des inneren Produkts

$$\langle f_{n_1}|f_{n_2}\rangle \;=\; \frac{1}{T}\int\limits_{T_0}^{T_0+T} n_2^{it}n_1^{-it}dt\,.$$

Es ist

$$\int\limits_{T_0}^{T_0+T}|S(it)|^2dt \;=\; \int\limits_{T_0}^{T_0+T}\left(\sum_{n_1=1}^{N}a_{n_1}n_1^{-it}\right)\left(\sum_{n_2=1}^{N}\overline{a_{n_2}}n_2^{it}\right)dt$$

$$=\sum_{1\le n_1,n_2\le N}a_{n_1}\overline{a_{n_2}}\int\limits_{T_0}^{T_0+T}\exp\left(it\log(\tfrac{n_2}{n_1})\right)dt \;=\; \Sigma_1+\Sigma_2$$

wobei wir in Σ_1 über die Diagonalterme mit $n_1=n_2$, und in Σ_2 über die anderen Terme mit $n_1\neq n_2$ summieren. Es ist offensichtlich

$$\Sigma_1 \;=\; T\cdot\sum_{n=1}^{N}|a_n|^2\,.$$

Es genügt daher zu zeigen:

$$(1)\qquad \sum_{1\le n_1<n_2\le N}a_{n_1}\overline{a_{n_2}}\int\limits_{T_0}^{T_0+T}\exp\left(it\log(\tfrac{n_2}{n_1})\right)dt \;\ll\; N\log(N)\sum_{n=1}^{N}|a_n|^2\,.$$

Es ist

$$\int\limits_{T_0}^{T_0+T}\exp\left(it\log(\tfrac{n_2}{n_1})\right)dt \;=\; O\left(|\log(\tfrac{n_2}{n_1})|^{-1}\right)\,.$$

Daher ist wegen $|a_{n_1}\overline{a_{n_2}}|\le|a_{n_1}|^2+|a_{n_2}|^2$:

$$\Sigma_2 \;\ll\; \sum_{1\le n_1\le N}|a_{n_1}|^2\cdot\sum_{\substack{1\le n_2\le N\\ n_2\neq n_1}}\left|\log(\tfrac{n_2}{n_1})\right|^{-1}\,.$$

Wir setzen $n_2=n_1+h$ und erhalten

$$\left|\log(\tfrac{n_2}{n_1})\right|^{-1} \;\ll\; \frac{N}{h}\,,\text{also}$$

$$\sum_{\substack{1\le n_2\le N\\ n_2\neq n_1}}\left|\log(\tfrac{n_2}{n_1})\right|^{-1} \;\ll\; N\log(N)\,.$$

Damit folgt (1). □

Satz 1.11.1 kann dazu verwendet werden, Aussagen über das quadratische Mittel von Dirichletreihen im Bereich ihrer absoluten Konvergenz zu machen. Der folgende Satz entspricht der Parsevalschen Gleichung für Fourierreihen:

Satz 1.11.2
Es sei $\sigma_0 \in \mathbb{R}$ fest. Die Dirichletreihe

$$D(s) \;=\; \sum_{n=1}^{\infty} a_n n^{-s}$$

sei absolut konvergent für $s = \sigma_0 + it$, $t \in \mathbb{R}$. Dann gilt

$$\lim_{T\to\infty} \frac{1}{2T} \int_{-T}^{T} |D(\sigma_0 + it)|^2 dt \;=\; \sum_{n=1}^{\infty} |a_n|^2 n^{-2\sigma_0}\,.$$

Beweis
Es sei $1 > \varepsilon > 0$ gegeben. Dann gibt es wegen der absoluten Konvergenz ein $N = N(\varepsilon)$, so dass

$$\sum_{n>N} |a_n| n^{-\sigma_0} \;<\; \varepsilon\,. \tag{1}$$

Damit folgt für genügend großes N auch

$$\sum_{n>N} |a_n|^2 n^{-2\sigma_0} \;<\; \varepsilon\,. \tag{2}$$

Nun ist

$$\int_{-T}^{T} |D(\sigma_0 + it)|^2 dt \;=\; \int_{-T}^{T} \left| \sum_{n=1}^{N} a_n n^{-(\sigma_0+it)} + R(t) \right|^2 dt$$

mit einem Restglied $R(t)$ mit $|R(t)| < \varepsilon$ für alle t wegen der absoluten Konvergenz. Es folgt

$$\left| \int_{-T}^{T} |D(\sigma_0 + it)|^2 dt \;-\; \int_{-T}^{T} \left| \sum_{n=1}^{N} a_n n^{-(\sigma_0+it)} \right|^2 dt \right| \;\le\; 4\varepsilon T \left(\sum_{n=1}^{N} |a_n| n^{-\sigma_0} \right) + 2\varepsilon^2 T\,. \tag{3}$$

Nach Satz 1.11.1 ist

$$\lim_{T\to\infty} \frac{1}{2T} \int_{-T}^{T} \left| \sum_{n=1}^{N} a_n n^{-(\sigma_0+it)} \right|^2 dt \;=\; \sum_{n=1}^{N} |a_n|^2 n^{-2\sigma_0}\,.$$

□

Kann die durch die Dirichletreihe $D(s) = \sum a_n n^{-s}$ definierte holomorphe Funktion in ein Gebiet links von der absoluten Konvergenzabszisse fortgesetzt werden, so können häufig auch dort noch Aussagen über das quadratische Mittel gemacht werden.

Satz 1.11.3
Für $\sigma_0 > \frac{1}{2}$, $\sigma_0 \neq 1$ gilt:

$$\lim_{T\to\infty} \frac{1}{2T} \int_{-T}^{T} |\zeta(\sigma_0 + it)|^2\, dt \;=\; \sum_{n=1}^{\infty} n^{-2\sigma_0}\,.$$

Beweis
Die Behauptung folgt für $\sigma_0 > 1$ sofort aus Satz 1.11.2, es sei also $\frac{1}{2} < \sigma_0 < 1$. Wir setzen $J = \max\{j \mid T \cdot 2^{-j} \ge T^{\frac{1}{3}}\}$. Für $0 \le j \le J$ sei $T_j = T \cdot 2^{-j}$. Es sei $T_j < t \le T$ beliebig, und stets $s = \sigma_0 + it$. Wir wenden die approximative Funktionalgleichung 1.8.5

$$\zeta(s) \;=\; \sum_{n\le x_j} n^{-s} \;+\; \chi(s) \sum_{n\le y_j(t)} n^{s-1} \;+\; O\left(x_j^{-\sigma_0} \log|t|\right) \;+\; O\left(|t|^{\frac{1}{2}-\sigma_0} y_j(t)^{\sigma_0-1}\right)$$

an und wählen $x_j = T_j^{\frac{3}{2}-\sigma_0}$ sowie $y_j = y_j(t) = \frac{t}{2\pi x_j}$. Für $\frac{1}{2}T_j < t \le T_j$ gilt dann

$$|\chi(s)| \;<\; T_j^{\frac{1}{2}-\sigma_0} \;\;,\;\; \left|\sum_{n\le y_j(t)} n^{s-1}\right| \underset{\sigma_0}{\ll} y_j(t)^{\sigma_0} \;\ll\; T_j^{\sigma_0\cdot(\sigma_0-\frac{1}{2})}\,.$$

Es gibt also ein $\delta = \delta(\sigma_0) > 0$, so dass

$$\zeta(s) \;=\; \sum_{n\le x_j} n^{-s} \;+\; R(s) \quad,\quad R(s) \underset{\delta,\sigma_0}{\ll} T_j^{-\delta}\,.$$

Es folgt

$$\left|\int\limits_{\frac{1}{2}T_j}^{T_j} |\zeta(\sigma_0+it)|^2\,dt \;-\; \int\limits_{\frac{1}{2}T_j}^{T_j}\left|\sum_{n\le x_j} n^{-s}\right|^2 dt\right| \;\ll\; \int\limits_{\frac{1}{2}T_j}^{T_j}\left|\sum_{n\le x_j} n^{-\sigma_0+it}\right|\cdot|R(\sigma_0+it)|\,dt \;+\; \int\limits_{\frac{1}{2}T_j}^{T_j}|R(\sigma_0+it)|^2\,dt$$

$$\underset{\delta,\sigma_0}{\overset{\text{Cauchy}}{\overset{\text{Schwarz}}{\ll}}} T_j^{-\delta}\left(\int\limits_{\frac{1}{2}T_j}^{T_j}\left|\sum_{n\le x_j} n^{-(\sigma_0+it)}\right|^2 dt\right)^{\frac{1}{2}}\cdot\left(\int\limits_{\frac{1}{2}T_j}^{T_j} 1dt\right)^{\frac{1}{2}} \underset{\delta,\sigma_0}{\ll} T_j^{\frac{1}{2}-\delta}\left(T_j + x_j\log(x_j)\right)^{\frac{1}{2}}\cdot\left(\sum_{n\le x_j} n^{-2\sigma_0}\right)^{\frac{1}{2}}$$

nach Satz 1.11.1. Also ist

$$\int\limits_{\frac{1}{2}T_j}^{T_j} |\zeta(\sigma_0+it)|^2\,dt \;=\; \int\limits_{\frac{1}{2}T_j}^{T_j}\left|\sum_{n\le x_j} n^{-(\sigma_0+it)}\right|^2 dt \;+\; O_{\delta,\sigma_0}\left(T_j^{1-\delta}\right)\,.$$

Wieder nach Satz 1.11.1 folgt

$$\int\limits_{\frac{1}{2}T_j}^{T_j} |\zeta(\sigma_0+it)|^2\,dt \;=\; \left(\tfrac{1}{2}T_j + O\left(x_j\log(x_j)\right)\right)\cdot\sum_{n\le x_j} n^{-2\sigma_0}\,. \tag{1}$$

Auf

$$\int\limits_{-2T_j^{\frac{1}{3}}}^{2T_j^{\frac{1}{3}}} |\zeta(\sigma_0+it)|^2\,dt$$

wenden wir die Hardy-Littlewood-Approximation (Satz 1.8.3) an, und erhalten $\zeta(\sigma_0+it) \ll T^{\frac{1}{6}}$ für $-2T^{\frac{1}{3}} \le t \le 2T^{\frac{1}{3}}$, also

$$\int\limits_{-2T^{\frac{1}{3}}}^{2T^{\frac{1}{3}}} |\zeta(\sigma_0+it)|^2\,dt \;\ll\; T^{\frac{2}{3}}\,. \tag{2}$$

Wir summieren die Beziehung (1) über j für $0 \le j \le J$ und erhalten mit (2) die Behauptung. □

1.12. Nullstellendichteabschätzungen

Das schärfste Restglied im Primzahlsatz erhält man unter Annahme der Riemannschen Vermutung

$$\zeta(\sigma+it) \;=\; 0 \text{ für } 0<\sigma<1 \quad\Longrightarrow\quad \sigma \;=\; \tfrac{1}{2}\,, \tag{RH}$$

d. h. alle nichttrivialen Nullstellen von $\zeta(s)$ liegen auf der kritischen Geraden. Während die Riemannsche Vermutung bis heute unbewiesen ist, ist seit 1913 (Bohr und Landau) bekannt, dass die meisten Nullstellen sehr nahe bei der kritischen Geraden liegen. Um dies zu präzisieren treffen wir

DEFINITION 1.12.1
Es sei $T > 0$ und $N(T) = \#\{\varrho = \beta + i\gamma \mid \zeta(\varrho) = 0\,,\ 0 \le \beta \le 1\,,\ 0 \le \gamma \le T\}$. Für $\frac{1}{2} \le \alpha \le 1$ sei

$$N(\alpha, T) \ = \ \#\{\varrho = \beta + i\gamma \mid \zeta(\varrho) = 0\,,\ \beta > \alpha\,,\ 0 < \gamma \le T\}\ .$$

Jede Nullstelle werde gemäß ihrer Vielfachheit gezählt.

Es wurde von Riemann vermutet und von v. Mangoldt (1894) bewiesen, dass

$$N(T) \ = \ \tfrac{T}{2\pi}\log\left(\tfrac{T}{2\pi}\right) \ - \ \tfrac{T}{2\pi} \ + \ O\left(\log(T)\right) \quad , \quad T \longrightarrow \infty\,.$$

Die Riemannsche Vermutung lässt sich formulieren als $N(\alpha, T) = 0$ für alle $\alpha \ge \frac{1}{2}$, während aus dem Ergebnis von Bohr und Landau folgt:

$$\forall \alpha \ge \tfrac{1}{2}: \ \lim_{T\to\infty} \frac{N(\alpha, T)}{N(T)} \ = \ 0\,. \tag{1}$$

Seither sind zahlreiche Ergebnisse über $N(\alpha, T)$ - so genannte Nullstellendichteabschätzungen - bewiesen worden, von denen wir eine hier wiedergeben wollen. Die Grundidee ist die Verwendung der approximativen Inversen $M_X(s)$ von $\zeta(s)$:

DEFINITION 1.12.2
Für $X \ge 1$ sei

$$M_X(s) \ = \ \sum_{n\le X} \mu(n) n^{-s} \quad , \quad f_X(s) \ = \ \zeta(s)\cdot M_X(s) - 1\,.$$

Für $\sigma > 1$ ist

$$\lim_{X\to\infty} M_X(s) \ = \ \sum_{n=1}^{\infty} \mu(n) n^{-s} \ = \ \zeta(s)^{-1} \ \text{ bzw. } \ \lim_{X\to\infty} f_X(s) \ = \ 0\,. \tag{2}$$

Es ist nicht bekannt, ob die unendliche Reihe (2) für $\sigma < 1$ konvergiert. Ihre Konvergenz für $\sigma > \frac{1}{2}$ ist äquivalent zur Riemannschen Vermutung. Jedoch kann gezeigt werden, dass für geeignetes X die Funktion $f_X(s)$ für die meisten $s = \sigma + it$ mit $\sigma > \frac{1}{2}$ klein ist. Andererseits ist $f_X(\varrho) = -1$, falls $\zeta(\varrho) = 0$ ist.

SATZ 1.12.1
Es sei $X = X(\sigma, T) \ge 1$ und $l(\sigma)$ eine monoton fallende und differenzierbare Funktion mit $|l'(\sigma)| \le C$. Es sei $m \ge 0$ und

$$\int_{\frac{1}{2}T}^{T} |f_X(s)|^2 dt \ \ll \ T^{l(\sigma)} \cdot (\log(T))^m$$

gleichmäßig für $\sigma \ge \alpha$. Dann ist

$$N(\sigma, T) \ \ll \ T^{l(\sigma)} \cdot \log^{m+3}(T)$$

für $\sigma \ge \alpha + \frac{1}{\log(T)}$.

BEWEIS
Es sei N_j die Menge aller Nullstellen $\varrho = \beta + i\gamma$ von $\zeta(s)$ mit $\beta \ge \sigma_0 \ge \alpha + \frac{1}{\log(T)}$ und $\frac{1}{2}T_j < \gamma \le T_j$ mit $T_j = T \cdot 2^{-j}$. Wir wählen eine „Teilmenge mit Minimalabstand“ $\{\varrho_1, \ldots, \varrho_R\} \subseteq N_j$ wie folgt aus: Es sei

$$\gamma_1 \ = \ \min\left\{\gamma \mid \beta + i\gamma \in N_j\,,\ \gamma \ge \tfrac{1}{2}T_j + 1\right\} \quad , \quad \varrho_1 \ = \ \beta_1 + i\gamma_1 \text{ mit } \beta_1 \text{ minimal gewählt}\,.$$

Ist $\varrho_{l-1} = \beta_{l-1} + i\gamma_{l-1} \in N_j$ schon definiert, so sei

$$\gamma_l \;=\; \min\{\gamma \mid \gamma \geq \gamma_{l-1}+1\,,\ \beta+i\gamma \in N_j \text{ für ein } \beta\} \quad,\quad \varrho_l \;=\; \beta_l + i\gamma_l \text{ mit } \beta_l \text{ minimal gewählt}\,.$$

Nach Satz 8.5.10 und Korollar 8.5.11 aus Funktionentheorie II gibt es $\ll \log(T_j)$ Nullstellen $\varrho = \beta+i\gamma$ von $\zeta(s)$ mit $\gamma_{l-1} < \gamma \leq \gamma_{l-1}+1$. Daher gilt

$$|N_j| \;\ll\; R \cdot \log(T_j)\,, \tag{1}$$

$$\gamma_{l+1} - \gamma_l \;\geq\; 1\,. \tag{2}$$

Die Idee für den Rest des Beweises ist die Folgende: In jeder Nullstelle ϱ_l für $1 \leq l \leq R$ ist $|f_X(\varrho_l)|^2$ groß. Dann ist $|f_X(s)|^2$ groß für s nahe bei ϱ_l. Die obere Schranke für

$$\int\limits_{\sigma_0 - \frac{1}{\log(T)}}^{1} \int\limits_{\frac{1}{2}T_j}^{T_j} |f_X(\sigma+it)|^2 dt d\sigma$$

bedingt, dass die Anzahl R klein sein muss. Versionen dieser Idee haben viele weitere Anwendungen, beispielsweise im Großen Sieb. Für $1 \leq l \leq R$ sei

$$K_l \;=\; \left\{ s \mid |s-\varrho_l| \leq \tfrac{1}{\log(T)} \right\}$$

die Kreisscheibe um den Mittelpunkt ϱ_l mit Radius $\frac{1}{\log(T)}$. Wegen (2) sind die K_l disjunkt. Nach der Cauchyschen Integralformel haben wir für $r \leq \frac{1}{\log(T)}$

$$f_X^2(\varrho_l) \;=\; \frac{1}{2\pi i} \int\limits_{|s-\varrho_l|=r} \frac{f_X^2(s)}{s-\varrho_l} ds\,,$$

also mit $s = \varrho_l + r\cos(\theta) + ir\sin(\theta)$ für $0 \leq \theta \leq 2\pi$:

$$|f_X^2(\varrho_l)| \;\leq\; \frac{1}{2\pi} \int\limits_0^{2\pi} |f_X(\varrho_l + r\cos(\theta) + ir\sin(\theta))|^2 \, d\theta$$

und

$$|f_X^2(\varrho_l)| \;\leq\; 2\log(T) \int\limits_{\frac{1}{2\log(T)}}^{\frac{1}{\log(T)}} \int\limits_0^{2\pi} r\,|f_X(\varrho_l + r\cos(\theta) + ir\sin(\theta))|^2 \, d\theta dr\,,$$

nach Übergang zu kartesischen Koordinaten also

$$|f_X^2(\varrho_l)| \;\leq\; 2\log(T) \iint\limits_{K_l} |f_X(\sigma+it)|^2 \, d\sigma dt\,.$$

Da die K_l paarweise disjunkt sind, folgt nach Annahme

$$\sum_{1 \leq l \leq R} \left| f_X^2(\varrho_l) \right| \;\ll\; \log(T) \int\limits_{\sigma_0 - \frac{1}{\log(T)}}^{1} \int\limits_{\frac{1}{2}T_j}^{T_j} |f_X(\sigma+it)|^2 dt d\sigma \;\ll\; T^{l(\sigma_0)} \cdot \log(T)^{m+1}\,. \tag{3}$$

Aus $\zeta(\varrho_l) = 0$ folgt $f_X(\varrho_l) = \zeta(\varrho_l) M_X(\varrho_l) - 1 = -1$. Also mit (3): $R \ll T_j^{l(\sigma_0)} \log(T)^{m+1}$. Wegen (1) folgt $|N_j| \ll T^{l(\sigma_0)} \log(T)^{m+2}$. Summieren über j liefert schließlich die Behauptung. $\square$

LEMMA 1.12.2
Für $c > 0$ gelte die Abschätzung $\zeta(\frac{1}{2}+it) = O_c(t^c)$, dann ist

$$\int_0^T |f_X(\tfrac{1}{2}+it)|^2 dt \underset{c}{\ll} T^{2c} \cdot (T+X) \cdot \log(X) .$$

BEWEIS
Es ist

$$|f_X(\tfrac{1}{2}+it)|^2 \le 2\left(|\zeta(\tfrac{1}{2}+it)|^2 \cdot |M_X(\tfrac{1}{2}+it)|^2 + 1\right) .$$

Nach Satz 1.11.1 ist

$$\int_0^T |M_X(\tfrac{1}{2}+it)|^2 dt \ll (T+X) \cdot \log(X) .$$

□

LEMMA 1.12.3
Für $T \ge e$ sei $1 + \frac{1}{2\log(T)} < \sigma_T \le 1 + \frac{2}{\log(T)}$. Es sei $1 \le X \le T$, dann ist

$$\int_0^T |f_X(\sigma_T + it)|^2 dt \ll \frac{T}{X} \cdot \log(T)^6 .$$

BEWEIS
Wir wenden die Hardy-Littlewood-Approximation 1.8.3 an:

$$\zeta(s) = \sum_{n \le x} n^{-s} - \frac{x^{1-s}}{1-s} + O_{\sigma_0, C}\left(x^{-\sigma}\right)$$

für $\sigma \ge \sigma_0 > 0$ und $|t| < \frac{2\pi x}{C}$, und erhalten mit $\sigma_0 = \frac{1}{2}$ und $x = T$

$$\zeta(s) = \zeta_T(s) + O\left(|t|^{-1}\right) \text{ mit } \zeta_T(s) = \sum_{n \le T} n^{-s} .$$

Also

$$f_X(s) = \zeta_T(s) M_X(s) - 1 + O\left(|M_X(s)| \cdot t^{-1}\right) \tag{1}$$

für $t \ge 1$. Nun ist

$$\zeta_T(s) \cdot M_X(s) = \sum_{1 \le n \le XT} b(n) n^{-s}$$

mit

$$b(n) = \sum_{\substack{d_1 \le X \\ d_2 \le T \\ d_1 d_2 = n}} \mu(d_1) .$$

Aus

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{falls} \quad n = 1 \\ 0 & \text{sonst} \end{cases}$$

folgt

$$b(n) = \begin{cases} 1 & \text{falls} \quad n = 1 \\ 0 & \text{falls} \quad n \le \min(X, T) \\ 0 & \text{falls} \quad n > XT \end{cases}$$

sowie

$$|b(n)| \le \tau(n) \tag{2}$$

für die Teilerfunktion $\tau(n)$. Es sei $X_j = X \cdot 2^j$ und $2^{J-1} < T \leq 2^J$, dann ist

$$\int_1^T |\zeta_T(s)M_X(s) - 1|^2 dt \ \ll \ \log(T)^2 \sum_{0 \leq j \leq J} \int_1^T \left| \sum_{x_j < n \leq 2x_j} b(n) n^{-(\sigma_T + it)} \right|^2 dt \, . \tag{3}$$

Nach Satz 1.11.1 ist

$$\int_1^T \left| \sum_{x_j < n \leq 2x_j} b(n) n^{-(\sigma_T + it)} \right|^2 dt \ \ll \ (T + x_j \log(x_j)) \ \cdot \sum_{x_j < n \leq 2x_j} |b(n)|^2 n^{-2\sigma_T} \, .$$

Übungsaufgabe 25 zeigt

$$\sum_{n \leq x} \tau(n)^2 \ \ll \ x \cdot \log(x)^3 \, . \tag{4}$$

Wegen (2), (3) und (4) gilt

$$\int_1^T |\zeta_T(s)M_X(s) - 1|^2 dt \ \ll \ \frac{T}{X} \cdot \log(T)^6 \, . \tag{5}$$

Andererseits ist

$$\int_1^T t^{-1} |M_X(s)| dt \ \ll \sum_{j \colon 1 \leq 2^j \leq T} \left(\int_{2^j}^{2^{j+1}} |M_X(\sigma_T + it)|^2 dt \right)^{\frac{1}{2}} \cdot \left(\int_{2^j}^{2^{j+1}} \frac{dt}{t^2} \right)^{\frac{1}{2}} \ \ll \ \log(T)^6 \, . \tag{6}$$

Aus (5) und (6) folgt die Behauptung. □

Aus den Abschätzungen für das quadratische Mittel auf den Geraden $s = \frac{1}{2} + it$ (Lemma 1.12.2) und $s = \sigma_T + it$ (Lemma 1.12.3) lässt sich nun mittels des folgenden Konvexitätsprinzips auch eine Abschätzung des quadratischen Mittels für die dazwischen liegenden Geraden $\alpha = \sigma + it$, $\frac{1}{2} \leq \sigma \leq 1$, gewinnen.

Lemma 1.12.4
Die Funktion f sei im Streifen $\sigma_1 \leq \sigma \leq \sigma_2$ holomorph und beschränkt. Es existiere

$$J(\sigma) \ = \ \int_{-\infty}^{\infty} |f(\sigma + it)|^2 dt \, ,$$

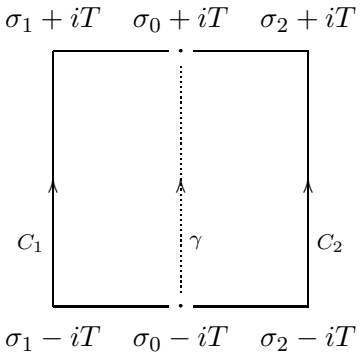
und sei gleichmäßig konvergent in $\sigma_1 \leq \sigma \leq \sigma_2$. Ferner gelte

$$\lim_{|t| \to \infty} |f(s)| \ = \ 0$$

gleichmäßig in $\sigma_1 \leq \sigma \leq \sigma_2$. Dann gilt

$$J(\sigma) \ \leq \ J(\sigma_1)^{\frac{\sigma_2 - \sigma}{\sigma_2 - \sigma_1}} \cdot J(\sigma_2)^{\frac{\sigma - \sigma_1}{\sigma_2 - \sigma_1}} \, .$$

Beweis
Wir betrachten den Spezialfall $\sigma_0 = \frac{1}{2}(\sigma_1 + \sigma_2)$, für den die Aussage die Form $J(\sigma_0) \leq J(\sigma_1)^{\frac{1}{2}} \cdot J(\sigma_2)^{\frac{1}{2}}$ annimmt. Für jedes $T > 0$ ist mit $f(s)$ auch die Spiegelung an der Mittelabszisse $f^*(s) = \overline{f(2\sigma_0 - \bar{s})}$ im Rechteck R mit den Eckpunkten $\sigma_{1,2} \pm iT$ holomorph (was man mit Hilfe der Charakterisierung der komplexen Differenzierbarkeit über die Cauchy-Riemannschen Differentialgleichungen schnell nachprüft). Wir ergänzen das fragliche Wegstück $\gamma = [\sigma_0 - iT, \sigma_0 + iT]$ auf zwei Arten zu einem geschlossenen Integrationsweg in R: Es sei C_1 die linke Randhälfte von R (negativ durchlaufen) und C_2 die rechte Randhälfte (positiv durchlaufen):



Auf der Abszisse σ_0 ist $f^*(s) = \overline{f(\bar{s})}$, also gilt

$$\int_\gamma f(s)f^*(s)ds \;=\; \int_\gamma |f(s)|^2 ds \;=\; \int_{-T}^{T} |f(\gamma(t))|^2\gamma'(t)dt \;=\; i\cdot\int_{-T}^{T} |f(\sigma_0+it)|^2 dt\,.$$

Auch $f\cdot f^*$ ist auf R holomorph, also ist das Integral nach dem Cauchyschen Integralsatz unabhängig vom Integrationsweg:

$$(1)\qquad \int_{C_1} f(s)f^*(s)ds \;=\; \int_{C_2} f(s)f^*(s)ds \;=\; \int_\gamma f(s)f^*(s)ds \;=\; i\cdot\int_{-T}^{T} |f(\sigma_0+it)|^2 dt\,.$$

Nach der Cauchy-Schwarzschen Ungleichung gilt

$$(2)\qquad \left|\int_{C_2} f(s)f^*(s)ds\right| \;\le\; \int_{C_2} |f(s)|\cdot|f^*(s)||ds| \;\le\; \left(\int_{C_2}|f(s)|^2|ds|\cdot\int_{C_2}|f^*(s)|^2|ds|\right)^{\frac12}$$

$$= \left(\int_{C_2}|f(s)|^2|ds|\right)^{\frac12}\cdot\left(\int_{C_1}|f(s)|^2|ds|\right)^{\frac12},$$

wobei im letzten Schritt benutzt wurde, dass $s\in C_2 \Leftrightarrow 2\sigma_0-\bar{s}\in C_1$ gilt. Aus der Voraussetzung $|f(s)|\to 0$ für $|t|\to\infty$ gleichmäßig in σ folgt, dass die Integrale über die horizontalen Wegstücke im Grenzwert verschwinden:

$$\lim_{T\to\infty}\int_{\sigma_0-iT}^{\sigma_1-iT}|f(s)|^2|ds| \;=\; \lim_{T\to\infty}\int_{\sigma_1+iT}^{\sigma_0+iT}|f(s)|^2|ds| \;=\; \lim_{T\to\infty}\int_{\sigma_0-iT}^{\sigma_2-iT}|f(s)|^2|ds| \;=\; \lim_{T\to\infty}\int_{\sigma_2+iT}^{\sigma_0+iT}|f(s)|^2|ds| \;=\; 0\,,$$

woraus

$$J(\sigma_j) \;=\; \int_{-\infty}^{\infty}|f(\sigma_j+it)|^2dt \;=\; \lim_{T\to\infty}\int_{C_j}|f(s)|^2|ds|$$

für $j=1,2$ folgt. Für $T\to\infty$ ergeben (1) und (2) damit die Konvexitätsaussage $J(\sigma_0)\le J(\sigma_1)\cdot J(\sigma_2)$ im Spezialfall $\sigma_0=\frac12(\sigma_1+\sigma_2)$. Nun sei $M\subseteq[\sigma_1,\sigma_2]$ die Menge aller σ, für die

$$J(\sigma) \;\le\; J(\sigma_1)^{\frac{\sigma_2-\sigma}{\sigma_2-\sigma_1}}\cdot J(\sigma_2)^{\frac{\sigma-\sigma_1}{\sigma_2-\sigma_1}}\,.$$

gilt. Wir haben $\sigma_0\in M$ schon gezeigt, und trivialerweise ist $\sigma_1,\sigma_2\in M$. Da σ_1 und σ_2 beliebig waren folgt, dass mit $a<b$ aus M auch der Mittelpunkt $c=\frac12(a+b)$ in M liegt, denn aus

$$a,b\in M \;\;\Rightarrow\;\; J(a) \;\le\; J(\sigma_1)^{\frac{\sigma_2-a}{\sigma_2-\sigma_1}}\cdot J(\sigma_2)^{\frac{a-\sigma_1}{\sigma_2-\sigma_1}}\,,\; J(b) \;\le\; J(\sigma_1)^{\frac{\sigma_2-b}{\sigma_2-\sigma_1}}\cdot J(\sigma_2)^{\frac{b-\sigma_1}{\sigma_2-\sigma_1}}\,,$$

folgt nach der obigen Rechnung

$$J(c) \;\le\; J(a)^{\frac{b-c}{b-a}} \cdot J(b)^{\frac{c-a}{b-a}} \;\le\; \left(J(\sigma_1)^{\frac{\sigma_2-a}{\sigma_2-\sigma_1}} \cdot J(\sigma_2)^{\frac{a-\sigma_1}{\sigma_2-\sigma_1}}\right)^{\frac{b-c}{b-a}} \cdot \left(J(\sigma_1)^{\frac{\sigma_2-b}{\sigma_2-\sigma_1}} \cdot J(\sigma_2)^{\frac{b-\sigma_1}{\sigma_2-\sigma_1}}\right)^{\frac{c-a}{b-a}}$$

$$= J(\sigma_1)^{\frac{\sigma_2-a}{\sigma_2-\sigma_1}\cdot\frac{b-c}{b-a}+\frac{\sigma_2-b}{\sigma_2-\sigma_1}\cdot\frac{c-a}{b-a}} \cdot J(\sigma_2)^{\frac{a-\sigma_1}{\sigma_2-\sigma_1}\cdot\frac{b-c}{b-a}+\frac{b-\sigma_1}{\sigma_2-\sigma_1}\cdot\frac{c-a}{b-a}} = J(\sigma_1)^{\frac{\sigma_2-c}{\sigma_2-\sigma_1}} \cdot J(\sigma_2)^{\frac{c-\sigma_1}{\sigma_2-\sigma_1}}$$

und damit $c \in M$. Induktiv liegt dann auch $2^{-k}l\cdot(\sigma_2-\sigma_1)$ in M für alle $k \in \mathbb{N}$ und $l = 0 \dots 2^k$. Da M offenbar eine dichte Teilmenge von $[\sigma_1, \sigma_2]$ ist folgt $M = [\sigma_1, \sigma_2]$, denn $J(\sigma)$ ist eine stetige Funktion in σ wegen der Voraussetzung, dass das Integral gleichmäßig σ konvergiert. □

Aus Satz 1.12.1 und den Lemmata 1.12.2 bis 1.12.4 folgt schließlich

Satz 1.12.5
Aus der Schranke $\zeta(\frac{1}{2}+it) \ll t^c$ *folgt*

$$N(\sigma, T) \;\ll\; T^{2(1+2c)(1-\sigma)} \cdot (\log(T))^7$$

gleichmäßig für $\frac{1}{2} \le \sigma \le 1$.

Beweis: Übungsaufgabe

□

Korollar 1.12.6
Für alle $\varepsilon > 0$ *gilt*

$$N(\sigma, T) \underset{\varepsilon}{\ll} T^{(\frac{8}{3}+\varepsilon)(1-\sigma)} \log(T)^7$$

gleichmäßig für $\frac{1}{2} \le \sigma \le 1$.

Beweis
Dies folgt aus der Abschätzung $\zeta(\frac{1}{2}+it) \ll t^{\frac{1}{6}}\log(t)$, die sich als Spezialfall für $l = 3$ aus Satz 1.10.1 ergibt. □

Korollar 1.12.7
Aus der Lindelöfschen Vermutung $\zeta(\frac{1}{2}+it) \ll t^{\varepsilon}$ *folgt*

$$N(\sigma, T) \underset{\varepsilon}{\ll} T^{(2+\varepsilon)(1-\sigma)} \log(T)^7 .$$

Beweis
Das ist klar. □

2. Primzahlen in arithmetischen Progressionen

2.1. Dirichletcharaktere

Grundlegend für die Behandlung von Primzahlen in arithmetischen Progressionen ist die zahlentheoretische Funktion des Dirichletcharakters. Einen Dirichletcharakter χ mod q ($q \in \mathbb{N}$) kann - wie in der Einleitung ausgeführt - als Gruppenhomomorphismus

$$\chi : (\mathbb{Z} / q\mathbb{Z}) \longrightarrow (\mathbb{C}^*, \cdot)$$

aufgefasst werden, der stetig ist (wenn wir endliche Mengen mit der diskreten Topologie versehen, d. h. alle Teilmengen gelten als offen). Man kann daraus auch eine zahlentheoretische Funktion gewinnen durch die Definition

$$\hat{\chi}(n) \;=\; \begin{cases} \chi(n \bmod q) & \text{falls} \quad \mathrm{ggT}(q,n) = 1 \\ 0 & \text{falls} \quad \mathrm{ggT}(q,n) \neq 1 \end{cases} .$$

Dies führt zu folgender Definition (wir identifizieren im Folgenden χ und $\hat{\chi}$):

Definition 2.1.1
Es sei $q \in \mathbb{N}$. Ein Dirichletcharakter mod q ist eine zahlentheoretische Funktion $\chi : \mathbb{Z} \to \mathbb{C}^*$ mit folgenden Eigenschaften:

(i) Periodizität: $\chi(m) = \chi(m + kq)$ für alle $k \in \mathbb{Z}$,
(ii) Multiplikativität: $\chi(mn) = \chi(m)\chi(n)$ für alle $m, n \in \mathbb{Z}$,
(iii) Normierung: $|\chi(m)| = 1$ für $\mathrm{ggT}(m, q) = 1$ und $\chi(m) = 0$ falls $\mathrm{ggT}(m, q) \neq 1$.

Der Hauptcharakter χ_0 mod q ist

$$\chi_0(m) \;=\; \begin{cases} 1 & \text{falls} \quad \mathrm{ggT}(m,q) = 1 \\ 0 & \text{falls} \quad \mathrm{ggT}(m,q) \neq 1 \end{cases} .$$

Satz 2.1.1
Für $q \in \mathbb{N}$ bilden die Dirichletcharaktere mod q bzgl. der Multiplikation eine Gruppe mit $\varphi(q)$ Elementen und dem neutralem Element χ_0.

Beweis
Das Inverse des Charakters χ ist $\bar{\chi}$ (der konjugiert-komplexe Charakter). Nach Übungsaufgabe 7 bilden die Charaktere von $(\mathbb{Z}/q\mathbb{Z})^*$ eine Gruppe, die zu $(\mathbb{Z}/q\mathbb{Z})^*$ isomorph ist, insbesondere gibt es $|(\mathbb{Z}/q\mathbb{Z})^*| = \varphi(q)$ Charaktere mod q. □

Satz 2.1.2 (Orthogonalitätsrelationen)
Durchläuft m ein vollständiges Vertretersystem mod q (etwa $m = 1, \ldots, q$), so ist

(i) $$\sum_{m \bmod q} \chi(m) \;=\; \begin{cases} \varphi(q) & \text{falls} \quad \chi = \chi_0 \\ 0 & \text{falls} \quad \chi \neq \chi_0 \end{cases} .$$

Durchläuft andererseits χ alle Dirichletcharaktere mod q, so ist

(ii) $$\sum_{\chi \bmod q} \chi(m) \;=\; \begin{cases} \varphi(q) & \text{falls} \quad m \equiv 1 \bmod q \\ 0 & \text{falls} \quad m \not\equiv 1 \bmod q \end{cases} .$$

Daraus folgen die allgemeineren Relationen

(iii) $$\sum_{1 \leq m \leq q} \chi_1(m)\overline{\chi_2(m)} \;=\; \begin{cases} \varphi(q) & \text{falls} \quad \chi_1 = \chi_2 \\ 0 & \text{falls} \quad \chi_1 \neq \chi_2 \end{cases} ,$$

(iv) $$\sum_{\chi \bmod q} \chi(m_1)\overline{\chi(m_2)} \;=\; \begin{cases} \varphi(q) & \text{falls} \quad m_1 \equiv m_2 \bmod q \\ 0 & \text{falls} \quad m_1 \not\equiv m_2 \bmod q \end{cases} .$$

Beweis
Für $\chi = \chi_0$ ist (i) klar. Ist $\chi \neq \chi_0$, so existiert ein b mit $\mathrm{ggT}(b,q) = 1$ und $\chi(b) \neq 1$. Da mit m auch bm alle Reste mod q durchläuft ist

$$\chi(b) \sum_{m \bmod q} \chi(m) \;=\; \sum_{m \bmod q} \chi(bm) \;=\; \sum_{m \bmod q} \chi(m)\,,$$

also $\sum \chi(m) = 0$ wegen $\chi(b) \neq 1$. Die Aussage (ii) ist ebenfalls klar für $m \equiv 1 \bmod q$. Der Fall $m \not\equiv 1 \bmod q$ erfordert als schwierigsten Teil den Nachweis der Existenz eines $\chi \bmod q$ mit $\chi(m) \neq 1$. Hier wenden wir den Hauptsatz über endliche abelsche Gruppen an: Die Gruppe der zu q teilerfremden Restklassen ist isomorph zu einem direkten Produkt von zyklischen Gruppen Z_l:

$$(\mathbb{Z} \,/\, q\mathbb{Z})^* \;\cong\; Z_1 \,\times\, \cdots \,\times\, Z_r\,.$$

Es sei $|Z_l| = n_l$ und $Z_l = \{e_l, z_l, \ldots, z_l^{n_l-1}\}$. Dann sind sämtliche Charaktere $\chi_{j,l}$ von Z_l gegeben durch

$$\chi_{j,l} \;=\; e_{n_l}(j) \;=\; \exp\left(\tfrac{2\pi i j}{n_l}\right) \quad , \quad 0 \le j \le n_l - 1\,.$$

Sämtliche Charaktere von $Z_1 \times \cdots \times Z_l$ haben dann die Form

$$\chi((h_1,\ldots,h_r)) \;=\; \chi_{j_1,1}(h_1)\cdots\chi_{j_r,r}(h_r) \quad , \quad h_i \in Z_i\,.$$

Für $\vec{h} = (h_1,\ldots,h_r) \neq (e_1,\ldots,e_r)$ gibt es daher stets einen Charakter χ von $Z_1 \times \cdots \times Z_r$, so dass $\chi(\vec{h}) \neq 1$ ist. Ist also $m \not\equiv 1 \bmod q$, so gibt es $\chi_1 \bmod q$ mit $\chi_1(m) \neq 1$. Da mit χ auch $\chi_1\chi$ alle Dirichletcharaktere mod q durchläuft, folgt

$$\chi_1(m) \sum_{\chi \bmod q} \chi(m) \;=\; \sum_{\chi \bmod q} \chi_1(m)\chi(m) \;=\; \sum_{\chi \bmod q} (\chi_1\chi)(m) \;=\; \sum_{\chi \bmod q} \chi(m)\,.$$

Wegen $\chi_1(m) \neq 1$ folgt $\sum \chi(m) = 0$. Mit χ_1 und χ_2 ist auch $\chi_1\overline{\chi_2}$ ein Dirichletcharakter mod q, und es ist $\chi_1\overline{\chi_2} = \chi_0$ genau dann, wenn $\chi_1 = \chi_2$ ist, daraus folgt (iii). Weiter ist $\chi(m_2)\overline{\chi(m_2)} = 1$ für $\mathrm{ggT}(m_2,q) = 1$, da $\overline{\chi(m_2)} = \chi(m_2^{-1})$ ist (m_2^{-1} ist das Inverse von m_2 mod q). Also

$$\sum_{\chi \bmod m} \chi(m_1)\overline{\chi(m_2)} \;=\; \sum_{\chi \bmod m} \chi(m_1 m_2^{-1})\,.$$

Daraus folgt (iv). □

Die Orthogonalitätsrelation (iv) ermöglicht es, aus einer Zahlenfolge (a_n) die Indizes einer gewünschten Restklasse „herauszufiltern“:

Satz 2.1.3
Es sei $q \in \mathbb{N}$ mit $\mathrm{ggT}(l,q) = 1$ und $(a_n)_{n=1}^{\infty}$ eine Zahlenfolge. Dann gilt

$$\sum_{\substack{n \le x \\ n \equiv l \bmod q}} a_n \;=\; \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi(l)} A(x,\chi)$$

mit

$$A(x,\chi) \;=\; \sum_{n \le x} a_n \chi(n)$$

sowie

$$\sum_{\substack{n=1 \\ n \equiv l \bmod q}}^{\infty} a_n \;=\; \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi(l)} A(\chi)$$

mit

$$A(\chi) \;=\; \sum_{n=1}^{\infty} a_n \chi(n)$$

falls die entsprechenden unendlichen Reihen konvergieren.

Beweis
Es ist

$$\frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi(l)} A(x,\chi) \;=\; \sum_{n \le x} a_n \left(\frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi(l)} \chi(n) \right) \;=\; \sum_{\substack{n \le x \\ n \equiv l \bmod q}} a_n$$

nach Satz 2.1.2(iv). □

2.2. Dirichletsche L-Reihen, Primzahlen in arithmetischen Progressionen

Definition 2.2.1
Es sei $q \in \mathbb{N}$ und χ ein Dirichletcharakter mod q. Unter der Dirichletschen L-Reihe $L(s,\chi)$ zu χ versteht man

$$L(s,\chi) \;=\; \sum_{n=1}^{\infty} \chi(n) n^{-s} \,.$$

Satz 2.2.1
Es sei $q \in \mathbb{N}$ und χ ein Dirichletcharakter mod q. $L(s,\chi)$ ist für $\sigma > 1$ normal konvergent, und für $\chi \neq \chi_0$ sogar für $\sigma > 0$. $L(s,\chi)$ stellt für $\sigma > 1$ (bzw. $\sigma > 0$ für $\chi \neq \chi_0$) eine holomorphe Funktion dar. Für $\sigma > 1$ gilt die normal konvergente Eulerproduktdarstellung

$$L(s,\chi) \;=\; \prod_{p} \frac{1}{1 - \chi(p) p^{-s}} \,, \tag{1}$$

insbesondere ist $L(s,\chi) \neq 0$ für $\sigma > 1$. Im Fall $\chi = \chi_0$ ist

$$L(s,\chi_0) \;=\; \zeta(s) \cdot \prod_{p \mid q} \left(1 - p^{-s}\right) \,. \tag{2}$$

Daher kann $L(s,\chi_0)$ zu einer in $\sigma > 0$ meromorphen Funktion fortgesetzt werden.

Beweis
Mit partieller Summation gilt

$$\sum_{n=1}^{\infty} \chi(n) n^{-s} \;=\; \lim_{N \to \infty} \left(N^{-s} \sum_{n \le N} \chi(n) \right) \;-\; s \int_1^{\infty} \left(\sum_{n \le u} \chi(n) \right) u^{-s-1} du \,. \tag{3}$$

Für $\chi \neq \chi_0$ gilt

$$\sum_{n=1}^{q} \chi(n) \;=\; 0 \quad \Longrightarrow \quad \forall u : \left| \sum_{n \le u} \chi(n) \right| \;\le\; q \,.$$

Damit existiert die rechte Seite von (3) für $\sigma > 0$. Die Eulerproduktdarstellung wurde in Übungsaufgabe 24 aus Funktionentheorie II bewiesen. Es ist

$$\chi_0(p) \;=\; \begin{cases} 0 & \text{falls} \quad p \mid q \\ 1 & \text{falls} \quad p \nmid q \end{cases} \,,$$

also für $\sigma > 1$

$$L(s,\chi_0) \;=\; \prod_{p \nmid q} (1 - p^{-s})^{-1} \;=\; \prod_{p} (1 - p^{-s})^{-1} \prod_{p \mid q} (1 - p^{-s}) \;=\; \zeta(s) \cdot \prod_{p \mid q} (1 - p^{-s}) \,.$$

□

Definition 2.2.2
Es sei $q \in \mathbb{N}$ und χ ein Dirichletcharakter mod q. Wir setzen

$$\psi(x,\chi) \;=\; \sum_{n\le x} \Lambda(n)\chi(n) \quad , \quad \psi(x,q,l) \;=\; \sum_{\substack{n\le x \\ n\equiv l \bmod q}} \Lambda(n) \quad , \quad \pi(x,q,l) \;=\; \sum_{\substack{p\le x \text{ prim} \\ p\equiv l \bmod q}} 1\,.$$

Satz 2.2.2
Es ist

$$\psi(x,q,l) \;=\; \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi(l)}\psi(x,\chi)\,.$$

Beweis
Das ist gerade die Aussage von Satz 2.1.3. □

Wir formulieren ohne Beweis

Satz 2.2.3 (Primzahlsatz für arithmetische Progressionen)
Es sei $q \in \mathbb{N}$ fest und $\mathrm{ggT}(q,l) = 1$*, dann ist*

$$\lim_{x\to\infty} \frac{\pi(x,q,l)}{x/(\varphi(q)\cdot\log(x))} \;=\; 1\,.$$

Eine Möglichkeit, diesen Satz zu beweisen, ist, in sämtlichen Überlegungen, die zum Beweis des Primzahlsatzes (Satz 8.3.5 aus Funktionentheorie II) führten, die Riemannsche ζ-Funktion durch die Reihen $L(s,\chi)$ zu ersetzen. Jede der beiden Vorgehensweisen der Vorlesung Funktionentheorie II kann übertragen werden. Zum einen kann das Ergebnis von Satz 8.3.7 $\zeta(1+it) \neq 0$ auf Dirichletsche L-Reihen übertragen werden: $L(1+it,\chi) \neq 0$. Daraus folgt wie in Satz 8.3.10

$$\lim_{x\to\infty} \frac{\psi(x,\chi_0)-x}{x} \;=\; 0 \quad \text{sowie} \quad \lim_{x\to\infty} \frac{\psi(x,\chi)}{x} \;=\; 0 \text{ für } \chi \neq \chi_0\,.$$

Die andere Möglichkeit besteht in der Herleitung von expliziten Formeln. Zunächst wird die Koeffizientenformel

$$\psi(x) \;=\; \frac{1}{2\pi i}\int_{b-iT}^{b+iT} -\frac{\zeta'(s)}{\zeta(s)}\cdot\frac{x^s}{s}ds \;+\; O\left(\frac{x\log(x)^2}{T}\right) \quad , \quad x \notin \mathbb{N}$$

verallgemeinert zu

$$\psi(x,\chi) \;=\; \frac{1}{2\pi i}\int_{b-iT}^{b+iT} -\frac{L'(s,\chi)}{L(s,\chi)}\cdot\frac{x^s}{s}ds \;+\; O_q\left(\frac{x\log(x)^2}{T}\right) \quad , \quad x \notin \mathbb{N}\,.$$

Eine Verschiebung des Integrationswegs führt dann zu einer Verallgemeinerung der expliziten Formel (Satz 8.6.2) der Form

$$\psi(x,\chi) \;=\; E(\chi)\cdot x \;-\; \sum_{\substack{\varrho:\, L(\varrho,\chi)=0 \\ |\mathrm{Im}(\varrho)|\le T}} \frac{x^\varrho}{\varrho} \;+\; O_q\left(\frac{x\log(T)^2}{T\log(x)}\right) \;+\; O_q\left(\frac{x\log(x)^2}{T}\right) \quad , \quad x \;=\; m+\frac{1}{2}\,,\; m\in\mathbb{N}$$

mit

$$E(\chi) \;=\; \begin{cases} 1 & \text{falls} \quad \chi = \chi_0 \\ 0 & \text{falls} \quad \chi \neq \chi_0 \end{cases}\,.$$

Die Ergebnisse über nullstellenfreie Zonen und Nullstellendichte sind für festes q auf Dirichletsche L-Reihen übertragbar. Man vermutet die Gültigkeit der verallgemeinerten Riemannschen Vermutung

$$L(s,\chi) = 0 \text{ für } 0 \le \mathrm{Re}(s) \le 1 \;\;\Longrightarrow\;\; \mathrm{Re}(s) = \frac{1}{2}\,.$$

Der Beweis für $L(1+it,\chi) \neq 0$ folgt für $t \neq 0$ dem Beweis von Satz 8.3.7: Wir setzen $\chi(n)n^{-it} = e^{i\vartheta}$, dann ist für $\sigma > 1$

$$\begin{aligned} l(\sigma) &= 3\log|\zeta(\sigma)| + 4\log|L(\sigma+it,\chi)| + \log|L(\sigma+2it,\chi^2)| \\ &= \operatorname{Re}\left(\sum_{n=1}^{\infty} a_n n^{-\sigma}\left(3+4\cos(\vartheta)+\cos(2\vartheta)\right)\right) \geq 0 \end{aligned}$$

wegen $a_n \geq 0$ und $3+4\cos(\vartheta)+\cos(2\vartheta) = 2(1+\cos(\vartheta))^2 \geq 0$. Dagegen folgt aus $L(1+it,\chi) = 0$

$$l(\sigma) \underset{\sigma\to 1}{\longrightarrow} -\infty\,.$$

Eine besondere Schwierigkeit bereitet der Beweis von $L(1,\chi) \neq 0$. Diese Schwierigkeit wurde bereits von Dirichlet gemeistert. Er bewies 1834, dass $\pi(x,q,l) \to \infty$ für $x \to \infty$ ist, falls $\operatorname{ggT}(q,l) = 1$ gilt. Zum Beweis dieser Tatsache genügt es, die Dirichletschen L-Reihe nur für reelle Werte von s zu betrachten. Der Beweis verwendet also nur reelle Analysis.

2.3. Der Dirichletsche Primzahlsatz

Lemma 2.3.1
Es sei $q \in \mathbb{N}$, und $z(q)$ die Anzahl der Dirichletcharaktere χ mod q, für die $L(1,\chi) = 0$ ist (mit Vielfachheiten gezählt). Dann ist

$$\lim_{\sigma\to 1+}\left((\sigma-1)\cdot\sum_{n\equiv 1 \bmod q}\Lambda(n)n^{-\sigma}\right) = \frac{1}{\varphi(q)}(1-z(q))\,.$$

Beweis
Wir verwenden im Folgenden die Tatsache, dass $L(\sigma,\chi)$ für $\chi \neq \chi_0$ und $L(\sigma,\chi_0) - \frac{1}{\sigma-1}$ Taylorentwicklungen um den Punkt $\sigma_0 = 1$ besitzen. Dies folgt aus der Holomorphie dieser Funktionen (Satz 2.2.1), lässt sich jedoch auch mit reeller Analysis beweisen (worauf wir nicht eingehen wollen). Es ist für $\sigma > 1$

$$\sum_{n\equiv 1 \bmod q}\Lambda(n)n^{-\sigma} = \frac{1}{\varphi(q)}\sum_{\chi \bmod q}\left(-\frac{L'(\sigma,\chi)}{L(\sigma,\chi)}\right)\,. \tag{1}$$

Es gilt

$$L(\sigma,\chi) \neq 0 \implies \frac{L'(\sigma,\chi)}{L(\sigma,\chi)} = O(1)\ (\sigma\to 1+)\,. \tag{2}$$

$L(\sigma,\chi)$ habe eine Nullstelle der Vielfachheit m_χ in $\sigma_0 = 1$. Dann haben $L(\sigma,\chi)$ und $L'(\sigma,\chi)$ die Taylorentwicklungen

$$L(\sigma,\chi) = c_{m_\chi}(\sigma-1)^{m_\chi} + c_{m_\chi+1}(\sigma-1)^{m_\chi+1} + \cdots\quad,\quad L'(\sigma,\chi) = m_\chi c_{m_\chi}(\sigma-1)^{m_\chi-1} + \cdots$$

um $\sigma_0 = 1$ mit $c_{m_\chi} \neq 0$. Also gilt

$$\lim_{\sigma\to 1+}\left((\sigma-1)\cdot\left(-\tfrac{L'(\sigma,\chi)}{L(\sigma,\chi)}\right)\right) = -m_\chi\,. \tag{3}$$

Außerdem ist

$$\lim_{\sigma\to 1+}\left((\sigma-1)\cdot\left(-\tfrac{L'(\sigma,\chi_0)}{L(\sigma,\chi_0)}\right)\right) = 1\,. \tag{4}$$

Aus (1), (2), (3) und (4) folgt die Behauptung. □

Definition 2.3.1
Der Dirichletcharakter χ mod q heißt reell, falls $\chi(m) \in \mathbb{R}$ für alle $m \in \mathbb{Z}$ ist, ansonsten komplex.

Lemma 2.3.2
Es gilt für festes q:

(i) $L(1,\chi) = 0$ *für höchstens ein* χ *mod* q.
(ii) *Für komplexe* χ *ist* $L(1,\chi) \neq 0$.

Beweis
Wegen

$$\lim_{\sigma \to 1+} \left((\sigma - 1) \sum_{n \equiv 1 \bmod q} \Lambda(n) n^{-\sigma} \right) \geq 0$$

folgt Teil (i) aus Lemma 2.3.1. Aus $L(1,\chi) = 0$ folgt $L(1,\overline{\chi}) = 0$. Da $\chi \neq \overline{\chi}$ ist für komplexe χ folgt (ii) aus (i). □

Wir zeigen im Folgenden, dass $L(1,\chi) \neq 0$ auch für die reellen χ gilt.

Lemma 2.3.3
Es sei $\chi \neq \chi_0$ *und* χ *reell, dann gilt*

$$\left| L(1,\chi) - \sum_{n \leq x} \chi(n) n^{-1} \right| \underset{q}{\ll} x^{-1} \tag{1}$$

und

$$\left| L(\tfrac{1}{2},\chi) - \sum_{n \leq x} \chi(n) n^{-\frac{1}{2}} \right| \underset{q}{\ll} x^{-\frac{1}{2}} . \tag{2}$$

Beweis
Es sei $\sigma > 0$. Abelsche partielle Summation ergibt

$$\left| L(\sigma,\chi) - \sum_{n \leq x} \chi(n) n^{-\sigma} \right| = \sigma \int_x^\infty \left(\sum_{x < n \leq u} \chi(n) \right) u^{-s-1} du \underset{q}{\ll} x^{-\sigma} .$$

□

Lemma 2.3.4
Für $\chi \neq \chi_0$ *reell ist* $L(1,\chi) \neq 0$.

Beweis
Es sei

$$F(n) = \sum_{d|n} \chi(d) .$$

F ist multiplikativ. Wir untersuchen die Werte von F für Primzahlpotenzen p^ν:

$$F(p^\nu) = \sum_{0 \leq \nu' \leq \nu} \chi(p^{\nu'}) = \begin{cases} 1 & \text{falls} \quad p|q \\ \nu+1 & \text{falls} \quad \chi(p) = 1 \\ 0 & \text{falls} \quad \chi(p) = -1 \quad \text{und} \quad \nu \text{ ungerade} \\ 1 & \text{falls} \quad \chi(p) = -1 \quad \text{und} \quad \nu \text{ gerade} \end{cases} .$$

Es ist $F(p^\nu) \geq 0$, und $F(p^\nu) \geq 1$ für $2|\nu$, also

$$F(n) \geq 0 \quad , \quad F(m^2) \geq 1 . \tag{1}$$

Wir setzen

$$G(x) = \sum_{n \leq x} F(n) n^{-\frac{1}{2}} .$$

Aus (1) folgt

$$G(x) \geq \sum_{m \leq x^{\frac{1}{2}}} F(m^2) m^{-1} \geq \sum_{m \leq x^{\frac{1}{2}}} m^{-1} > \frac{1}{2} \log(x) . \tag{2}$$

Andererseits ist

$$(3) \qquad G(x) \;=\; \sum_{n\le x} n^{-\frac{1}{2}} \sum_{d\mid n} \chi(d) \;=\; \sum_{d\le x^{\frac{1}{2}}} \chi(d) d^{-\frac{1}{2}} \sum_{d'\le \frac{x}{d}} (d')^{-\frac{1}{2}} \;+\; \sum_{d'\le x^{\frac{1}{2}}} (d')^{-\frac{1}{2}} \sum_{x^{\frac{1}{2}}<d\le \frac{x}{d'}} \chi(d) d^{-\frac{1}{2}} \,.$$

Nach der Eulerschen Summenformel ist für $\sigma > 0$ dann

$$\sum_{n\le y} n^{-\sigma} \;=\; \int_1^y u^{-\sigma} du \;-\; \sigma \int_1^y B_0(u) u^{-\sigma-1} du \;-\; y^{-\sigma} B_0(y) \;+\; B_0(1) \,.$$

Wegen

$$\int_1^y B_0(u) u^{-\sigma-1} du \;=\; \int_1^\infty B_0(u) u^{-\sigma-1} du \;+\; O_\sigma\left(y^{-\sigma}\right)$$

folgt mit einer passenden Konstanten $C = C(\sigma)$

$$(4) \qquad \sum_{n\le y} n^{-\sigma} \;=\; (1-\sigma)^{-1} y^{-\sigma+1} \;+\; C(\sigma) \;+\; O_\sigma\left(y^{-\sigma}\right) \,.$$

Aus Lemma 2.3.3 sowie (3) und (4) folgt

$$G(x) \;=\; \sum_{d\le x^{\frac{1}{2}}} \chi(d) d^{-\frac{1}{2}} \left(2\left(\tfrac{x}{d}\right)^{\frac{1}{2}} + C(\tfrac{1}{2}) + O\left(\left(\tfrac{d}{x}\right)^{\frac{1}{2}}\right)\right) \;+\; \sum_{d'\le x^{\frac{1}{2}}} \left((d')^{-\frac{1}{2}} \cdot O(x^{-\frac{1}{4}})\right)$$

$$= \left(2L(1,\chi) + O(x^{-\frac{1}{2}})\right) \cdot x^{\frac{1}{2}} \;+\; C(\tfrac{1}{2}) \cdot \left(L(\tfrac{1}{2},\chi) + O(x^{-\frac{1}{4}})\right) \;+\; O(1) \,.$$

Man sieht, dass die Annahme $L(1,\chi) = 0$ zu $G(x) = O(1)$ führt, ein Widerspruch zu (2). □

Satz 2.3.5
Es sei $q \in \mathbb{N}$ und $\mathrm{ggT}(q,l) = 1$, dann ist

$$\lim_{\sigma\to 1+} \left((\sigma-1) \cdot \left(\sum_{n\equiv l \bmod q} \Lambda(n) n^{-\sigma}\right)\right) \;=\; \frac{1}{\varphi(q)} \,.$$

Insbesondere enthält die arithmetische Progression $l \bmod q$ unendlich viele Primzahlen.

Beweis
Die Lemmata 2.3.2 und 2.3.4 implizieren $z(q) = 0$ in Lemma 2.3.1, woraus die Behauptung folgt. □

3. Die Kreismethode von Hardy und Littlewood

3.1. Einleitung

Ein Grundproblem der additiven Zahlentheorie ist von folgender Art: es seien $\mathbb{N}_i$ endlich (oder abzählbar unendlich) viele Mengen nichtnegativer ganzer Zahlen. M sei eine weitere Menge ganzer Zahlen. Was kann über die Darstellungen der Form

$$n_1 + n_2 + \cdots + n_r \;=\; N \quad n_i \in \mathbb{N}_i \,,\; N \in M \tag{1}$$

ausgesagt werden? Zur Behandlung dieser Fragen haben Hardy und Littlewood ihre Kreismethode entwickelt. Für jede Menge $\mathbb{N}_i$ wird eine erzeugende Funktion

$$f_i(z) \;=\; \sum_{n \in \mathbb{N}_i} z^n$$

eingeführt. Wegen $\mathbb{N}_i \subseteq \mathbb{N} \cup \{0\}$ sind die Potenzreihen $f_i(z)$ absolut konvergent für $|z| < 1$. Es sei $r(N)$ die Anzahl der Darstellungen von N in der Form (1). Dann ist nach der Cauchyschen Integralformel für $R < 1$

$$r(N) \;=\; \frac{1}{2\pi i} \int\limits_{|z|=R} \left(\prod_{i \in I} f_i(z) \right) z^{-(N+1)} dz \,. \tag{2}$$

Die Methode hat ihren Namen also von der Wahl des Integrationswegs, den Kreis mit Radius R. In vielen Fällen lässt sich nun das Integral (2) für $R \to 1$ asymptotisch auswerten. Später hat Vinogradoff die Kreismethode abgewandelt, indem er die Kreise $|z| = R$ durch den Einheitskreis $|z| = 1$ und diesen mittels der Substitution $z = e(\alpha)$ durch das Einheitsintervall $[0, 1]$ ersetzt hat. Die unendlichen Reihen $f_i(z)$, die für $|z| = 1$ nicht mehr zu konvergieren brauchen, werden - endliche Indexmenge I vorausgesetzt - durch die endlichen Abschnitte

$$f_{i,N_i}(z) \;=\; \sum_{\substack{n \in \mathbb{N}_i \\ n \le N_i}} z^n \;=\; \sum_{\substack{n \in \mathbb{N}_i \\ n \le N_i}} e(n\alpha) \;=\; f_{i,N_i}(e(\alpha))$$

ersetzt. Die Formel (2) wird dann ersetzt durch

$$r(N) \;=\; \int\limits_0^1 \left(\prod_{i \in I} f_{i,N_i}(e(\alpha)) \right) e(-N\alpha) d\alpha \,. \tag{3}$$

In wichtigen Spezialfällen sind die Mengen $\mathbb{N}_i$ Wertemengen von Polynomen: $\mathbb{N}_i = \{P_i(n) \mid n \in \mathbb{N}\}$. Die Summen

$$f_{i,N_i}(e(\alpha)) \;=\; \sum_{\substack{n \in \mathbb{N}_i \\ n \le N_i}} e(\alpha P_i(n))$$

sind dann Weylsche Exponentialsummen. Die Methode der Auswertung von (3) ist grob wir folgt: wir teilen $[0, 1]$ in zwei Teilmengen ein für passend gewählte Parameter Q und η:

$$\mathcal{M}_1 \;=\; \bigcup_{\substack{q \le Q \\ 1 \le a < q \\ (a,q)=1}} \mathcal{M}(a, q) \quad , \quad \mathcal{M}_2 \;=\; [0, 1] \setminus \mathcal{M}_1 \,.$$

Dabei sind die Mengen $\mathcal{M}(a, q)$ Umgebungen rationaler Punkte $\frac{a}{q}$:

$$\mathcal{M}(a, q) \;=\; \left[\tfrac{a}{q} - \eta, \tfrac{a}{q} + \eta\right] \quad , \quad \mathcal{M}(0) \;=\; [0, \eta] \quad , \quad \mathcal{M}(1) \;=\; [1 - \eta, 1] \,.$$

Die Menge $\mathcal{M}_1$ besteht aus den so genannten major arcs $\mathcal{M}(a, q)$, und ist die Menge derjenigen α, die eine gute Diophantische Approximation $|\alpha - \frac{a}{q}| \le \eta$ durch Zahlen $\frac{a}{q}$ mit kleinem Nenner haben.

$\mathcal{M}_2$ besteht aus den minor arcs. Nach dem Dirichletschen Approximationssatz 1.3.1 besitzen auch die $\alpha \in \mathcal{M}_2$ eine Approximation der Form

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}\,, \tag{4}$$

der Nenner q ist hier aber größer. Für $\alpha \in \mathcal{M}_1$ wird der Integrand in (3) asymptotisch ausgewertet, während der Beitrag für $\alpha \in \mathcal{M}_2$ nach oben abgeschätzt wird. Grundlegend für diese Abschätzung sind eine Mittelwertaussage und die Weylsche Ungleichung 1.5.3, bei der eine Diophantische Approximation der Form (4) vorausgesetzt wird. In günstigen Fällen lässt sich dann beweisen, dass

$$\int\limits_{\mathcal{M}_1} \left(\prod_{i\in I} f_{i,N_i}(e(\alpha))\right) e(-N\alpha)dx$$

einen größeren Beitrag liefert als das Integral über $\mathcal{M}_2$, obwohl das Maß von $\mathcal{M}_1$ kleiner ist, als das Maß von $\mathcal{M}_2$. Wir werden als einziges Beispiel für dieses Verfahren das Waringsche Problem behandeln.

3.2. Das Waringsche Problem

Beim Waringschen Problem wird nach den Darstellungen von natürlichen Zahlen als Summe von k-ten Potenzen gefragt:

$$n_1^k + n_2^k + \cdots + n_r^k \;=\; n\,. \tag{1}$$

Waring vermutete 1770, dass es für alle k eine Zahl r gibt, so dass sich jede Zahl $n \in \mathbb{N}$ als Summe von r k-ten Potenzen schreiben lässt. Die Zahl r der in (1) benötigten Summanden ist also nicht unbeschränkt. $g(k)$ sei die kleinste Zahl mit dieser Eigenschaft für die k-ten Potenzen. Der Fall $k = 2$ wurde schon von Lagrange im 18. Jahrhundert gelöst: es ist $g(2) = 4$, d. h. jede natürliche Zahl ist eine Summe von 4 Quadraten ganzer Zahlen, während drei Quadrate nicht ausreichen. Das Waringsche Problem wurde vollständig von Hilbert im Jahr 1909 gelöst. An Stelle von $g(k)$ kann auch die Zahl $G(k)$ betrachtet werden: sie ist die kleinste Zahl r, so dass jede hinreichend große Zahl $n \in \mathbb{N}$ als Summe von r k-ten Potenzen geschrieben werden kann. Ziel dieses Abschnitts ist der Beweis des folgenden Satzes, aus dem $G(k) \leq 2^k + 1$ folgt:

Satz 3.2.1 (Hardy-Littlewood)
Es sei $k \geq 2$ und $s \geq 2^k + 1$. Es sei $r_{k,s}(N)$ die Anzahl der Darstellungen von N als Summe von s k-ten Potenzen natürlicher Zahlen. Dann gibt es eine multiplikative zahlentheoretische Funktion $\mathfrak{S}(N)$ und $\delta = \delta(k,s) > 0$, so dass

$$r_{k,s}(N) \;=\; \mathfrak{S}(N)\cdot\Gamma(1+\tfrac{1}{k})^s\cdot\Gamma(\tfrac{s}{k})^{-1}\cdot N^{\left(\frac{s}{k}-1\right)} \;+\; O_{k,s}\left(N^{\frac{s}{k}-1-\delta}\right)$$

gilt. Es gibt zudem positive Konstanten $c_1 = c_1(k,s)$ und $c_2 = c_2(k,s)$, so dass $c_1 < \mathfrak{S}(N) < c_2$ für alle N ist.

3.3. Zerlegung des Integrationsintervalls

Definition 3.3.1
Es sei $N \in \mathbb{N}$ und $N \geq 2^k$, $P = [N^{\frac{1}{k}}]$, sowie

$$F(\alpha) \;=\; \sum_{m=1}^{P} e(\alpha m^k)\,.$$

LEMMA 3.3.1
Es gilt

$$r_{k,s}(N) \;=\; \int_0^1 F(\alpha)^s e(-N\alpha)d\alpha\,.$$

BEWEIS
Klar. □

Wie in der Einleitung ausgeführt, zerlegen wir das Integrationsintervall in zwei Teilmengen $\mathcal{M}_1$ und $\mathcal{M}_2$, wobei $\mathcal{M}_1$ aus den major arcs, und $\mathcal{M}_2$ aus den minor arcs besteht.

DEFINITION 3.3.2
Es sei $0 \le \nu < \frac{1}{5}$, $1 \le q \le P^\nu$, $0 \le a \le q$ mit $\mathrm{ggT}(a,q) = 1$. Wir setzen

$$\mathcal{M}(a,q) \;:=\; \left\{\alpha \in [0,1] \mid \left|\alpha - \tfrac{a}{q}\right| \le \tfrac{1}{P^{k-\nu}}\right\}\,,$$

also

$$\mathcal{M}(a,q) \;=\; \left[\tfrac{a}{q} - \tfrac{1}{P^{k-\nu}}\,,\, \tfrac{a}{q} + \tfrac{1}{P^{k-\nu}}\right] \text{ für } q > 1\,,$$

$$\mathcal{M}(0,1) \;=\; \left[0, \tfrac{1}{P^{k-\nu}}\right] \;,\; \mathcal{M}(1,1) \;=\; \left[1 - \tfrac{1}{P^{k-\nu}}, 1\right]\,,$$

$$\mathcal{M}_1 \;=\; \bigcup_{1\le q\le P^\nu} \bigcup_{\substack{a=0\\(a,q)=1}}^{q} \mathcal{M}(a,q)\,.$$

LEMMA 3.3.2
Die major arcs sind paarweise disjunkt, d. h. für $\frac{a}{q} \ne \frac{a'}{q'}$ *ist* $\mathcal{M}(a,q) \cap \mathcal{M}(a',q') = \emptyset$. $\mathcal{M}_1$ *hat eine Länge*

$$l(\mathcal{M}_1) \;\le\; \frac{2}{P^{k-3\nu}}\,.$$

BEWEIS
Es sei $\alpha \in \mathcal{M}(a,q) \cap \mathcal{M}(a',q')$ mit $\frac{a}{q} \ne \frac{a'}{q'}$, dann ist $|aq' - a'q| \ge 1$ und

$$\frac{1}{P^{2\nu}} \;\le\; \frac{1}{qq'} \;\le\; \left|\frac{a}{q} - \frac{a'}{q'}\right| \;\le\; \left|\alpha - \frac{a}{q}\right| + \left|\alpha - \frac{a'}{q'}\right| \;\le\; \frac{2}{P^{k-\nu}}\,.$$

Dies ist für $P \ge 2$ und $k \ge 2$ unmöglich. Die Länge von $\mathcal{M}(0,1) \cup \mathcal{M}(1,1)$ ist $2P^{\nu-k}$. Für jedes $q \ge 2$ und $\mathrm{ggT}(a,q) = 1$ ist $l(\mathcal{M}(a,q)) = 2P^{\nu-k}$. Für jedes $q \ge 2$ gibt es genau $\varphi(q)$ Zahlen $1 \le a \le q$ mit $\mathrm{ggT}(a,q) = 1$, daher ist

$$l(\mathcal{M}_1) \;=\; \frac{2}{P^{k-\nu}} \sum_{1\le q\le P^\nu} \varphi(n) \;\le\; \frac{2}{P^{k-\nu}} \sum_{1\le q\le P^\nu} q \;\le\; \frac{2}{P^{k-\nu}} \cdot \frac{P^\nu(P^\nu+1)}{2} \;\le\; \frac{2}{P^{k-3\nu}}\,.$$

□

BEMERKUNG 3.3.1
Aus Lemma 3.3.2 ergibt sich $l(\mathcal{M}_1) \to 0$ und $l(\mathcal{M}_2) \to 1$ für $P \to \infty$.

Obwohl die Menge der major arcs $\mathcal{M}_1$ eine viel kleinere Länge hat als die Menge der minor arcs $\mathcal{M}_2$, ist in der Zerlegung

$$r_{k,s}(N) \;=\; \int_0^1 F(\alpha)^s e(-N\alpha)d\alpha \;=\; \int_{\mathcal{M}_1} F(\alpha)^s e(-N\alpha)d\alpha \;+\; \int_{\mathcal{M}_2} F(\alpha)^s e(-N\alpha)d\alpha$$

das erste Integral über $\mathcal{M}_1$ asymptotisch gleich dem Hauptglied von Satz 3.2.1:

$$\int\limits_{\mathcal{M}_1} F(\alpha)^s e(-N\alpha)d\alpha \ \sim \ \mathfrak{S}(N)\Gamma(1+\tfrac{1}{k})^s\Gamma(\tfrac{s}{k})^{-1}N^{\left(\frac{s}{k}\right)^{-1}} ,$$

während

$$\int\limits_{\mathcal{M}_2} F(\alpha)^s e(-N\alpha)d\alpha \ \underset{k,s}{\ll} \ N^{\frac{s}{k}-1-\delta}$$

nur zum Restglied beiträgt. Zunächst werden wir den Beitrag der minor arcs abschätzen.

3.4. Die Minor Arcs

Satz 3.4.1
Es sei $k \geq 2$ und $s \geq 2^k + 1$, dann gibt es $\delta_1 = \delta_1(k,s) > 0$ mit

$$\int\limits_{\mathcal{M}_2} F(\alpha)^s e(-N\alpha)d\alpha \ \underset{k,s}{\ll} \ N^{\frac{s}{k}-1-\delta_1} .$$

Der Beweis beruht auf der Weylschen Ungleichung 1.5.3 und auf Hua's Lemma, einer Mittelwertaussage, die wir zuerst behandeln:

Lemma 3.4.2 (Hua)
Für $k \geq 2$ und $\varepsilon > 0$ ist

$$\int\limits_0^1 |F(\alpha)|^{2^k} d\alpha \ \underset{k,\varepsilon}{\ll} \ P^{2^k-k+\varepsilon} .$$

Beweis
Wir beweisen durch Induktion nach l, dass

$$\int\limits_0^1 |F(\alpha)|^{2^l} d\alpha \ \underset{l,\varepsilon}{\ll} \ P^{2^l-l+\varepsilon} \tag{1}$$

für $1 \leq l \leq k$ gilt.

<u>$l = 1$:</u>

$$\int\limits_0^1 |F(\alpha)|^2 d\alpha \ = \ \sum_{m=1}^{P}\sum_{n=1}^{P}\int\limits_0^1 e(\alpha(m^k - n^k))d\alpha \ = \ P$$

ist die Parsevalsche Gleichung.

<u>$l \to l+1$ $(l \leq k-1)$:</u>
Wir wenden Lemma 1.2.3 an: Es ist

$$F(\alpha) \ = \ S(f) \ = \ \sum_{n=1}^{p} e(f(n))$$

mit $f(x) = \alpha x^k$. Nach Lemma 1.2.3 ist

$$|F(\alpha)|^{2^l} \ = \ |S(f)|^{2^l} \ \leq \ (2P+1)^{2^l-l-1} \sum_{|d_1|\leq P} \cdots \sum_{|d_l|\leq P} S_{d_l,\ldots,d_1}(f) \tag{2}$$

mit

$$S_{d_l,\dots,d_1}(f) \;=\; \sum_{n\in I(d_l,\dots,d_1)} e\left(\Delta_{d_l,\dots,d_1}(f)(n)\right)\;,$$

wobei $I(d_l,\dots,d_1)$ ein Intervall von aufeinander folgenden Zahlen ist, das in $[1,P]$ liegt. Durch Induktion nach l zeigt man leicht, dass

$$\Delta_{d_l,\dots,d_1}(f)(x) \;=\; \alpha d_l\cdots d_1 Q_{k-l}(x)$$

ist mit einem Polynom $Q_{k-l}(x)$ vom Grad $k-l$ und ganzzahligen Koeffizienten. Nach (2) folgt

$$|F(\alpha)|^{2^l} \;\le\; (2P+1)^{2^l-l-1}\sum_{|d_1|\le P}\cdots\sum_{|d_l|\le P}\sum_{n\in I(d_l,\dots,d_1)} e\left(\alpha d_l\cdots d_1 Q_{k-l}(n)\right) \tag{3}$$

$$\le\; (2P+1)^{2^l-l-1}\sum_d r(d)e(\alpha d)\;,$$

wobei $r(d)$ die Anzahl der Faktorisierungen von d in der Form $d=d_l\cdots d_1Q_{k-l}(n)$ mit $|d_i|\le P$ und $n\in I(d_l,\dots,d_1)$ ist. Wegen $d\ll P^k$ folgt nach Lemma 1.4.2

$$r(d) \;\ll\; |d|^{\varepsilon} \;\ll\; P^{\varepsilon} \tag{4}$$

für $d\neq 0$. Da $Q_{k-l}(x)=0$ für höchstens $k-l$ ganze Zahlen x ist, folgt

$$r(0)\ll P^l\;. \tag{5}$$

Andererseits gilt

$$|F(\alpha)|^{2^l} \;=\; F(\alpha)^{2^{l-1}}\cdot F(-\alpha)^{2^{l-1}} \;=\; \left(\sum_{m=1}^{P} e(-\alpha m^k)\right)^{2^{l-1}}\cdot\left(\sum_{n=1}^{P} e(\alpha n^k)\right)^{2^{l-1}}$$

$$=\sum_{m_1=1}^{P}\cdots\sum_{m_{2^{l-1}}=1}^{P}\sum_{n_1=1}^{P}\cdots\sum_{n_{2^{l-1}}=1}^{P} e\left(\alpha\cdot\left(\sum_{i=1}^{2^{l-1}} n_i^k-\sum_{i=1}^{2^{l-1}} m_i^k\right)\right) \;=\; \sum_d s(d)e(-\alpha d)\;,$$

wobei $s(d)$ die Anzahl der Darstellungen von d in der Form

$$d \;=\; \sum_{i=1}^{2^{l-1}} m_i^k \;-\; \sum_{i=1}^{2^{l-1}} n_i^k \quad,\quad 1\le m_i,n_i\le P$$

für $i=1,\dots,l-1$ ist. Dann ist

$$\sum_d s(d) \;=\; |T(0)|^{2^l} \;=\; P^{2^l} \tag{6}$$

und nach Induktionsannahme

$$s(0) \;=\; \int_0^1 |T(0)|^{2^l}\,d\alpha \;\ll\; P^{2^l-l+\varepsilon}\;. \tag{7}$$

Mit (3), (4), (5), (6) und (7) folgt, dass

$$\int_0^1 |F(\alpha)|^{2^{l+1}}d\alpha \;=\; \int_0^1 |F(\alpha)|^{2^l}|F(\alpha)|^{2^l}d\alpha \;\le\; (2P+1)^{2^l-l-1}\int_0^1\sum_{d'} r(d')e(\alpha d')\sum_d s(d)e(-\alpha d)d\alpha$$

$$=\;(2P+1)^{2^l-l-1}\sum_d r(d)s(d) \;=\; (2P+1)^{2^l-l-1}r(0)s(0) \;+\; (2P+1)^{2^l-l-1}\sum_{d\neq 0} r(d)s(d)$$

$$\underset{l,\varepsilon}{\ll} P^{2^l-l-1}\cdot P^l\cdot P^{2^l-l+\varepsilon} + P^{2^l-l-1}\cdot P^\varepsilon\sum_{d\neq 0} s(d) \ll P^{2^{l+1}-(l+1)+\varepsilon} + P^{2^l-l-1}\cdot P^\varepsilon\sum_{d\neq 0} s(d)$$

$$\ll P^{2^{l+1}-(l+1)+\varepsilon} + P^{2^l-l-1}\cdot P^\varepsilon\cdot P^{2^l} \ll P^{2^{l+1}-(l+1)+\varepsilon}.$$

□

Beweis von Satz 3.4.1
Nach dem Dirichletschen Approximationssatz 1.3.1 gibt es für alle $\alpha\in\mathbb{R}$ und $N\in\mathbb{N}$ Zahlen $a\in\mathbb{Z}$ und $q\in\mathbb{N}$ mit $1\leq q\leq N$ und $|\alpha-\frac{a}{q}|\leq\frac{1}{qN}$. Wir wenden dies für $\alpha\in\mathcal{M}_2$ und $N=P^{k-\nu}$ an und erhalten (a,q) mit $1\leq q\leq P^{k-\nu}$ und $\mathrm{ggT}(a,q)=1$, sowie

$$\left|\alpha-\frac{a}{q}\right| \leq \frac{1}{qP^{k-\nu}} \leq \min\left(\tfrac{1}{P^{k-\nu}},\tfrac{1}{q^2}\right).$$

Aus $q\leq P^\nu$ folgt $|\alpha-\frac{a}{q}|\leq\frac{1}{P^{k-\nu}}$, also $\alpha\in\mathcal{M}_1$, ein Widerspruch. Daher ist $P^\nu<q\leq P^{k-\nu}$. Aus der Weylschen Ungleichung 1.5.3 folgt

$$(1)\quad F(\alpha)\underset{k,\varepsilon}{\ll} P^{1+\varepsilon}\left(P^{-1}+q^{-1}+P^{-k}q\right)^{\frac{1}{K}} \ll P^{1+\varepsilon}\left(P^{-1}+q^{-1}+P^{-k}P^{k-\nu}\right)^{\frac{1}{K}} \ll P^{1+\varepsilon-\frac{\nu}{K}}$$

mit $K=2^{k-1}$. Aus (1) und Hua's Lemma 3.4.2 folgt

$$\left|\int_{\mathcal{M}_2} F(\alpha)^s e(-N\alpha)d\alpha\right| = \left|\int_{\mathcal{M}_2} F(\alpha)^{s-2^k}F(\alpha)^{2^k}e(-N\alpha)d\alpha\right|$$

$$\leq \int_{\mathcal{M}_2}|F(\alpha)|^{s-2^k}|F(\alpha)|^{2^k}d\alpha \leq \max_{\alpha\in\mathcal{M}_2}|F(\alpha)|^{s-2^k}\cdot\int_0^1|F(\alpha)|^{2^k}d\alpha$$

$$\ll \left(P^{1+\varepsilon-\frac{\nu}{K}}\right)^{s-2^k}\cdot P^{2^k-k+\varepsilon} = P^{s-k-\delta_1}$$

mit

$$\delta_1 = \frac{\nu(s-2^k)}{K}-(s-2^k+1)\varepsilon > 0$$

für hinreichend kleines ε. Damit ist Satz 3.4.1 bewiesen. □

3.5. Die Major Arcs

Definition 3.5.1
Wir setzen

$$v(\beta) = v(N,\beta) = \sum_{m=1}^{N}\frac{1}{k}m^{\frac{1}{k}-1}e(\beta m) \quad , \quad S(a,q) = \sum_{\nu=1}^{q} e\left(\tfrac{a\nu^k}{q}\right).$$

Lemma 3.5.1
Es sei $|\beta|\leq\frac{1}{2}$. Dann ist

$$(1)\qquad v(\beta)\underset{k}{\ll}\min\left(P,\,|\beta|^{-\frac{1}{k}}\right).$$

Beweis
Es gilt

$$|v(\beta)| \ \leq \ \sum_{m=1}^{N} \frac{1}{k} m^{\frac{1}{k}-1} \ \leq \ \int_{1}^{N} k^{-1} x^{\frac{1}{k}-1} dx + 1 \ \leq \ N^{\frac{1}{k}} \ \ll \ P \, .$$

Ist $|\beta| \leq \frac{1}{N}$, so ist $P \leq N^{\frac{1}{k}} \leq |\beta|^{-\frac{1}{k}}$, und $v(\beta) \ll \min(P, |\beta|^{-\frac{1}{k}})$, also (1). Wir können also annehmen, dass $\frac{1}{N} < |\beta| \leq \frac{1}{2}$ gilt. Dann ist $|\beta|^{-\frac{1}{k}} \ll P$. Es sei $M = [|\beta|^{-1}]$, dann ist $M \leq \frac{1}{|\beta|} < M + 1 \leq N$. Es sei

$$U(t) \ = \ \sum_{m \leq t} e(\beta m) \quad , \quad f(t) \ = \ \frac{1}{k} \cdot t^{\frac{1}{k}-1} \, .$$

Nach Lemma 1.2.1 ist $U(t) \ll \|\beta\|^{-1} = |\beta|^{-1}$. Partielle Summation ergibt

$$\sum_{M < m \leq N} \frac{1}{k} m^{\frac{1}{k}-1} e(\beta m) \ = \ [f(t)U(t)]_{M}^{N} - \int_{M}^{N} U(t) f'(t) dt \ \ll \ |\beta|^{-1} M^{\frac{1}{k}-1} \ \leq \ |\beta|^{-\frac{1}{k}} \ \ll \ \min\left(P, |\beta|^{-\frac{1}{k}}\right) .$$

Deshalb ist

$$v(\beta) \ = \ \sum_{m=1}^{M} \frac{1}{k} m^{\frac{1}{k}-1} e(\beta m) \ + \ \sum_{m=M+1}^{N} \frac{1}{k} m^{\frac{1}{k}-1} e(\beta m) \ \ll \ \min\left(P, |\beta|^{-\frac{1}{k}}\right) .$$

□

Lemma 3.5.2
Es seien $\mathrm{ggT}(a,q) = 1$, $1 \leq q \leq P^{\nu}$ *und* $0 \leq a < q$. *Wenn* $\alpha \in \mathcal{M}(a,q)$ *ist, so gilt*

$$F(\alpha) \ = \ \left(\frac{S(a,q)}{q}\right) \cdot v(\alpha - \tfrac{a}{q}) \ + \ O(P^{2\nu}) \, .$$

Beweis
Es sei $\beta = \alpha - \frac{a}{q}$. Dann ist $|\beta| \leq P^{\nu-k}$ und

$$F(\alpha) - \frac{S(a,q)}{q} v(\beta) \ = \ \sum_{m=1}^{P} e(am^k) - \frac{S(a,q)}{q} \sum_{m=1}^{N} \frac{1}{k} m^{\frac{1}{k}-1} e(\beta m)$$

$$= \ \sum_{m=1}^{P} e\left(\tfrac{am^k}{q}\right) e(\beta m^k) - \frac{S(a,q)}{q} \sum_{m=1}^{N} \frac{1}{k} m^{\frac{1}{k}-1} e(\beta m) \ = \ \sum_{m=1}^{N} u(m) e(\beta m) \, ,$$

mit

$$u(m) \ = \ \begin{cases} e(\frac{am}{q}) - \frac{S(a,q)}{q} k^{-1} m^{\frac{1}{k}-1} & \text{falls} \quad m = n^k \\ -\frac{S(a,q)}{q} k^{-1} m^{\frac{1}{k}-1} & \text{sonst} \end{cases} .$$

Es sei $y \geq 1$. Da $|S(a,q)| \leq q$ ist haben wir

$$\sum_{1 \leq m \leq y} e\left(\frac{am^k}{q}\right) \ = \ \sum_{\nu=1}^{q} e\left(\frac{a\nu^k}{q}\right) \sum_{\substack{1 \leq m \leq y \\ m \equiv \nu \bmod q}} 1 \ = \ S(a,q) \cdot \left(\tfrac{y}{q} + O(1)\right) \ = \ y \cdot \left(\tfrac{S(a,q)}{q}\right) + O(q) \, .$$

Es sei $t \geq 1$. Da $v(\beta) \ll P$ ist folgt

$$U(t) \ = \ \sum_{1 \leq m \leq t} u(m) \ = \ \sum_{1 \leq m \leq t^{\frac{1}{k}}} e\left(\frac{am^k}{q}\right) - \frac{S(a,q)}{q} \sum_{1 \leq m \leq t} \frac{1}{k} m^{\frac{1}{k}-1}$$

$$= t^{\frac{1}{k}} \left(\frac{S(a,q)}{q} \right) + O(q) - \frac{S(a,q)}{q} \cdot \left(t^{\frac{1}{k}} + O(1) \right) = O(q) .$$

Partielle Integration ergibt

$$\sum_{m=1}^{N} u(m) e(\beta m) = e(\beta N) U(N) - 2\pi i \beta \int_1^N e(\beta t) U(t) dt$$

$$= O(q) - 2\pi i \beta \int_1^N e(\beta t) O(q) dt \ll q + |\beta| N q \ll (1 + |\beta| N) q \ll (1 + P^{\nu-k} P^k) P^\nu \ll P^{2\nu} .$$

Damit ist Lemma 3.5.3 bewiesen. □

LEMMA 3.5.3
Es sei

$$\mathfrak{S}(N, Q) = \sum_{1 \le q \le Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(\tfrac{S(a,q)}{q} \right)^s e(-N \tfrac{a}{q})$$

und

$$J^*(N) = \int_{-P^{\nu-k}}^{P^{\nu-k}} v(\beta)^s e(-N\beta) d\beta ,$$

dann ist

$$\int_{\mathcal{M}_1} F(\alpha)^s e(-N\alpha) d\alpha = \mathfrak{S}(N, P^\nu) \cdot J^*(N) + O\left(P^{s-k-\delta_2} \right)$$

mit $\delta_2 = 1 - 5\nu > 0$.

BEWEIS
Es sei $\alpha \in \mathcal{M}(a,q)$ und $\beta = \alpha - \frac{a}{q}$. Zudem sei

$$V = V(\alpha, a, q) = \frac{S(a,q)}{q} \cdot v(\alpha - \tfrac{a}{q}) = \frac{S(a,q)}{q} \cdot v(\beta) .$$

Da $|S(a,q)| \le q$ gilt, ist nach Lemma 3.5.1 $|V| \ll |v(\beta)| \ll P$. Es sei $F = F(\alpha)$, dann ist $|F| \le P$. Da nach Lemma 3.5.2 $F - V \ll P^{2\nu}$ ist folgt, dass

$$F^s - V^s = (F - V) \cdot \left(F^{s-1} + F^{s-2} V + \cdots + V^{s-1} \right) = P^{s-1+2\nu}$$

gilt. Da nach Lemma 3.3.2 $\mu(\mathcal{M}_1) \ll P^{3\nu-k}$ ist folgt, dass

$$\int_{\mathcal{M}_1} |F^s - V^s| \, d\alpha \ll P^{3\nu-k} \cdot P^{s-1+2\nu} = P^{s-k-\delta_2}$$

ist mit $\delta_2 = 1 - 5\nu > 0$. Es folgt

$$\int_{\mathcal{M}_1} F(\alpha)^s e(-N\alpha) d\alpha = \int_{\mathcal{M}_1} V(\alpha, a, q)^s e(-N\alpha) d\alpha + O\left(P^{s-k-\delta_2} \right) \tag{1}$$

$$= \sum_{1 \le q \le P^\nu} \sum_{\substack{a=0 \\ (a,q)=1}}^{q} \int_{\mathcal{M}(a,q)} V(\alpha, a, q)^s e(-N\alpha) d\alpha + O\left(P^{s-k-\delta_2} \right) .$$

Für $q \geq 2$ haben wir

$$\int\limits_{\mathcal{M}(a,q)} V(\alpha,a,q)^s e(-N\alpha)d\alpha \;=\; \int\limits_{\frac{a}{q}-P^{\nu-k}}^{\frac{a}{q}+P^{\nu-k}} V(\alpha,a,q)^s e(-N\alpha)d\alpha \tag{2}$$

$$= \int\limits_{-P^{\nu-k}}^{P^{\nu-k}} V(\beta+\tfrac{a}{q},a,q)^s e(-N(\beta+\tfrac{a}{q}))d\beta \;=\; \left(\frac{S(a,q)}{q}\right)^s \cdot e(-N\tfrac{a}{q}) \;\cdot \int\limits_{-P^{\nu-k}}^{P^{\nu-k}} v(\beta)^s e(-N\beta)d\beta$$

$$= \left(\frac{S(a,q)}{q}\right)^s \cdot e(-N\tfrac{a}{q}) \cdot J^*(N)\,.$$

Für $q = 1$ haben wir $V(\alpha,0,1) = v(\alpha)$ und $V(\alpha,1,1) = v(\alpha-1)$. Deshalb

$$\int\limits_{\mathcal{M}(0,1)} V(\alpha,a,q)^s e(-N\alpha)d\alpha + \int\limits_{\mathcal{M}(1,1)} V(\alpha,a,q)^s e(-N\alpha)d\alpha$$

$$= \int\limits_{0}^{P^{\nu-k}} v(\alpha)^s e(-N\alpha)d\alpha + \int\limits_{1-P^{\nu-k}}^{1} v(\alpha-1)^s e(-N\alpha)d\alpha$$

$$= \int\limits_{0}^{P^{\nu-k}} v(\beta)^s e(-N\beta)d\beta + \int\limits_{-P^{\nu-k}}^{0} v(\beta)^s e(-N\beta)d\beta\,.$$

Mit (1) und (2) folgt

$$\int\limits_{\mathcal{M}_1} F(\alpha)^s e(-N\alpha)d\alpha \;=\; \sum_{1\leq q\leq P^\nu} \sum_{\substack{a=1\\(a,q)=1}}^{q} \left(\tfrac{S(a,q)}{q}\right)^s \cdot e(-N\tfrac{a}{q}) \cdot J^*(N) + O\left(P^{s-k-\delta_2}\right)$$

$$= \mathfrak{S}(N,P^\nu) \cdot J^*(N) + O\left(P^{s-k-\delta_2}\right)\,.$$

□

3.6. Das singuläre Integral

Wir betrachten als nächstes das singuläre Integral

$$J(N) \;=\; \int\limits_{-\frac{1}{2}}^{\frac{1}{2}} v(\beta)^s e(-N\beta)d\beta\,.$$

Satz 3.6.1
Es gibt $\delta_3 > 0$, so dass

$$J(N) \underset{s,k}{\ll} P^{s-k} \text{ und } J^*(N) \;=\; J(N) + O\left(P^{s-k-\delta_3}\right)\,.$$

Beweis
Nach Lemma 3.5.1 ist

$$J(N) \underset{k}{\ll} \int_0^{\frac{1}{2}} \min\left(P, |\beta|^{-\frac{1}{k}}\right)^s d\beta = \int_0^{\frac{1}{N}} \min\left(P, |\beta|^{-\frac{1}{k}}\right)^s d\beta + \int_{\frac{1}{N}}^{\frac{1}{2}} \min\left(P, |\beta|^{-\frac{1}{k}}\right)^s d\beta$$

$$= \int_0^{\frac{1}{N}} P^s d\beta + \int_{\frac{1}{N}}^{\frac{1}{2}} \beta^{-\frac{s}{k}} d\beta \underset{k}{\ll} P^{s-k}$$

und

$$J(N) - J^*(N) = \int\limits_{P^{\nu-k} \le |\beta| \le \frac{1}{2}} v(\beta)^s e(-N\beta) d\beta \ll \int_{P^{\nu-k}}^{\frac{1}{2}} |v(\beta)|^s d\beta$$

$$\ll \int_{P^{\nu-k}}^{\frac{1}{2}} \beta^{-\frac{s}{k}} d\beta \ll P^{(k-\nu)(\frac{s}{k}-1)} = P^{s-k-\delta_3}$$

mit $\delta_3 = v(\frac{s}{k} - 1) > 0$. □

Lemma 3.6.2
Es seien α und β reell, so dass $0 < \beta < 1$ und $\alpha \ge \beta$ ist. Dann ist

$$\sum_{m=1}^{N-1} m^{\beta-1}(N-m)^{\alpha-1} = N^{\alpha+\beta-1} \cdot \frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)} + O_\beta(N^{\alpha-1}) .$$

Beweis
Es sei $g(x) = x^{\beta-1}(N-x)^{\alpha-1}$. Dann existiert das uneigentliche Integral

$$\int_0^N g(x)dx .$$

Es ist

$$\int_0^N g(x)dx = \int_0^N x^{\beta-1}(N-x)^{\alpha-1}dx = N^{\alpha+\beta-1}\int_0^1 t^{\beta-1}(1-t)^{\alpha-1}dt$$

$$= N^{\alpha+\beta-1}B(\alpha,\beta) = N^{\alpha+\beta-1}\frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)} .$$

Dabei ist

$$B(\alpha,\beta) = \int_0^1 t^{\beta-1}(1-t)^{\alpha-1}dt = \frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)}$$

die Eulersche Beta-Funktion. Ist $\alpha \ge 1$, so gilt

$$g'(x) = g(x) \cdot \left(\tfrac{\beta-1}{x} - \tfrac{\alpha-1}{N-x}\right) < 0 ,$$

d. h. $g(x)$ ist fallend auf $(0, N)$, und

$$\int_1^N g(x)dx < \sum_{m=1}^{N-1} g(m) < \int_0^{N-1} g(x)dx .$$

Deshalb ist

$$0 \;<\; \int_0^N g(x)dx - \sum_{m=1}^{N-1} g(m) \;<\; \int_0^1 g(x)dx \;=\; \int_0^1 x^{\beta-1}(N-x)^{\alpha-1}dx \;\le\; N^{\alpha-1}\int_0^1 x^{\beta-1}dx \;=\; \frac{N^{\alpha-1}}{\beta}\,.$$

Ist $0 < \beta \le \alpha < 1$, so ist $0 < \alpha + \beta < 2$ und $g(x)$ hat ein lokales Minimum im Punkt

$$c \;=\; \frac{(1-\beta)N}{2-\alpha-\beta} \;\in\; \left[\tfrac{N}{2}, N\right]\,.$$

Da $g(x)$ streng monoton fallend ist für $x \in (0, c)$, folgt

$$\sum_{m=1}^{[c]} g(m) \;<\; \int_0^c g(x)dx$$

sowie

$$\sum_{m=1}^{[c]} g(m) \;\ge\; \int_1^{[c]} g(x)dx + g([c]) \;>\; \int_1^c g(x)dx \;>\; \int_0^c g(x)dx - \frac{N^{\alpha-1}}{\beta}\,.$$

Ähnlich folgt, da $g(x)$ monoton wächst für $x \in (c, N)$

$$\sum_{m=[c]+1}^{N-1} g(m) \;<\; \int_c^N g(x)dx$$

sowie

$$\sum_{m=[c]+1}^{N-1} g(m) \;\ge\; \int_{[c]+1}^{N-1} g(x)dx + g([c]+1) \;>\; \int_c^{N-1} g(x)dx \;>\; \int_c^N g(x)dx - \frac{N^{\beta-1}}{\alpha}\,.$$

Deshalb ist

$$0 \;<\; \int_0^N g(x)dx - \sum_{m=1}^{N-1} g(m) \;<\; \frac{N^{\alpha-1}}{\beta} + \frac{N^{\beta-1}}{\alpha} \;\le\; \frac{2N^{\alpha-1}}{\beta}\,.$$

Dies beschließt den Beweis. □

Satz 3.6.3
Wenn $s \ge 2$ ist, gilt

$$J(N) \;=\; \Gamma\left(1+\tfrac{1}{k}\right)^s \cdot \Gamma\left(\tfrac{s}{k}\right)^{-1} \cdot N^{\frac{s}{k}-1} \;+\; O(N^{\frac{s-1}{k}-1})\,.$$

Beweis
Es sei

$$J_s(N) \;=\; \int_{-\frac{1}{2}}^{\frac{1}{2}} v(\beta)^s e(-N\beta)d\beta$$

für $s \ge 1$. Wir berechnen dieses Integral durch Induktion nach s:

$$v(\beta) \;=\; \sum_{m=1}^{N} \frac{1}{k} m^{\frac{1}{k}-1} e(m\beta)$$

folgt, dass

$$v(\beta)^s \;=\; \frac{1}{k^s} \sum_{m_1=1}^{N} \cdots \sum_{m_s=1}^{N} (m_1 \cdots m_s)^{\frac{1}{k}-1} e((m_1 + \cdots + m_s)\beta)$$

und deshalb

$$J_s(N) \;=\; \frac{1}{k^s}\sum_{m_1=1}^{N}\cdots\sum_{m_s=1}^{N}(m_1\cdots m_s)^{\frac{1}{k}-1}\int_{-\frac{1}{2}}^{\frac{1}{2}}e((m_1+\cdots+m_s-N)\beta)d\beta$$

$$=\;\frac{1}{k^s}\;\cdot\sum_{\substack{m_1+\cdots+m_s=N\\1\le m_j\le N}}(m_1+\cdots+m_s)^{\frac{1}{k}-1}\,.$$

Induktionsanfang $s=2$:
Wir wenden Lemma 3.6.2 mit $\alpha=\beta=\frac{1}{k}$ an, und erhalten

$$J_2(N) \;=\; \frac{1}{k^2}\sum_{m=1}^{N-1}m^{\frac{1}{k}-1}(N-m)^{\frac{1}{k}-1}$$

$$=\;\frac{(\frac{1}{k})^2\cdot\Gamma(\frac{1}{k})^2}{\Gamma(\frac{2}{k})}\cdot N^{\frac{2}{k}-1}\;+\;O(N^{\frac{1}{k}-1}) \;=\; \frac{\Gamma(1+\frac{1}{k})^2}{\Gamma(\frac{2}{k})}\cdot N^{\frac{2}{k}-1}\;+\;O(N^{\frac{1}{k}-1})\,.$$

Induktionsschritt $s\to s+1$:

$$J_{s+1}(N) \;=\; \int_{-\frac{1}{2}}^{\frac{1}{2}}v(\beta)^{s+1}e(-N\beta)d\beta \;=\; \int_{-\frac{1}{2}}^{\frac{1}{2}}v(\beta)v(\beta)^{s}e(-N\beta)d\beta$$

$$=\;\int_{-\frac{1}{2}}^{\frac{1}{2}}\sum_{m=1}^{N}\frac{1}{k}m^{\frac{1}{k}-1}e(m\beta)v(\beta)^s e(-N\beta)d\beta \;=\; \sum_{m=1}^{N}\frac{1}{k}m^{\frac{1}{k}-1}J_s(N-m)$$

$$=\;\frac{\Gamma(1+\frac{1}{k})^s}{\Gamma(\frac{s}{k})}\sum_{m=1}^{N-1}\frac{1}{k}m^{\frac{1}{k}-1}(N-m)^{\frac{s}{k}-1}\;+\;O\left(\sum_{m=1}^{N-1}\frac{1}{k}m^{\frac{1}{k}-1}(N-m)^{\frac{s-1}{k}-1}\right)\,.$$

Wir wenden nun Lemma 3.6.2 mit $\alpha=\frac{s}{k}$ und $\beta=\frac{1}{k}$ an und erhalten

$$\sum_{m=1}^{N-1}\frac{1}{k}m^{\frac{1}{k}-1}(N-m)^{\frac{s}{k}-1} \;=\; \frac{(\frac{1}{k})\cdot\Gamma(\frac{1}{k})\cdot\Gamma(\frac{s}{k})}{\Gamma(\frac{s+1}{k})}\cdot N^{\frac{s+1}{k}-1}\;+\;O(N^{\frac{s}{k}-1})\,.$$

Dies ergibt

$$J_{s+1}(N) \;=\; \frac{\Gamma(1+\frac{1}{k})^{s+1}}{\Gamma(\frac{s+1}{k})}\cdot N^{\frac{s+1}{k}-1}\;+\;O(N^{\frac{s}{k}-1})$$

und die Induktion ist abgeschlossen. □

3.7. Die singuläre Reihe

Definition 3.7.1
Es sei

$$A_N(q) \;=\; \sum_{\substack{a=1\\(a,q)=1}}^{q}\left(\tfrac{S(a,q)}{q}\right)^s\cdot e\left(\tfrac{-Na}{q}\right)\;\;,\;\;\mathfrak{S}(N) \;=\; \sum_{q=1}^{\infty}A_N(q)\,.$$

LEMMA 3.7.1
Es sei $0 < \varepsilon < \frac{1}{sK}$. *Es gibt* $\delta_4 = \delta_4(k,s) > 0$, *so dass* $A_n(q) \ll \frac{1}{q^{1+\delta_4}}$.

BEWEIS
Da $s \geq 2^k + 1 = 2K + 1$ ist haben wir

$$\frac{s}{K} - 1 - s\varepsilon \;\geq\; 1 + \frac{1}{K} - s\varepsilon \;=\; 1 + \delta_4$$

mit $\delta_4 = \frac{1}{K} - s\varepsilon > 0$. Nach der Weylschen Ungleichung 1.5.3 ist

$$A_N(q) \;\ll\; \frac{q}{q^{\frac{s}{K} - s\varepsilon}} \;\leq\; \frac{1}{q^{1+\delta_4}}\,.$$

□

LEMMA 3.7.2
Die singuläre Reihe

$$\mathfrak{S}(N) \;=\; \sum_{q=1}^{\infty} A_N(q)$$

konvergiert absolut und gleichmäßig in N. *Es gibt* $c = c(k,s)$ *mit*

$$|\mathfrak{S}(N)| \;<\; c \quad , \quad \mathfrak{S}(N) - \mathfrak{S}(N, P^\nu) \;\ll\; P^{-\nu\delta_4}\,.$$

BEWEIS
Das folgt sofort aus Lemma 3.7.1. □

Wir wollen im Folgenden zeigen, dass $0 < c_1 < \mathfrak{S}(N) < c_2$ gilt.

LEMMA 3.7.3
Es sei $\mathrm{ggT}(q,r) = 1$, *dann ist* $S(mr + nq, qr) = S(m,q) \cdot S(n,r)$.

BEWEIS
Der Beweis wurde in Übungsaufgabe 10 geführt. □

LEMMA 3.7.4 (Multiplikativität von A_N)
Es sei $\mathrm{ggT}(q,r) = 1$, *dann gilt* $A_N(qr) = A_N(q) \cdot A_N(r)$.

BEWEIS
Der Beweis verläuft ähnlich wie in Beispiel 0.0.6 (Multiplikativität der Ramanujan-Summe). Die Abbildung

$$(\mathbb{Z}\,/\,q\mathbb{Z})^* \;\times\; (\mathbb{Z}\,/\,r\mathbb{Z})^* \;\longmapsto\; (\mathbb{Z}\,/\,qr\mathbb{Z})^* \quad , \quad (m \bmod q, n \bmod r) \;\longmapsto\; (rm + qn) \bmod qr$$

ist eine Bijektion. Daher ist

$$A_N(qr) \;=\; \sum_{\substack{m=1 \\ (m,q)=1}}^{q} \sum_{\substack{n=1 \\ (n,r)=1}}^{r} \left(\tfrac{S(mr+nq,qr)}{qr}\right)^s \cdot e\left(-\tfrac{(mr+nq)N}{qr}\right)$$

$$= \sum_{\substack{m=1 \\ (m,q)=1}}^{q} \sum_{\substack{n=1 \\ (n,r)=1}}^{r} \left(\tfrac{S(m,q)}{q}\right)^s \cdot \left(\tfrac{S(n,r)}{r}\right)^s \cdot e\left(-\tfrac{mN}{q}\right) \cdot e\left(-\tfrac{nN}{r}\right) \;=\; A_N(q) \cdot A_N(r)\,.$$

□

LEMMA 3.7.5 (Eulerprodukt der singulären Reihe)
Es ist

$$\mathfrak{S}(N) \;=\; \prod_{p\,\text{prim}} \left(1+\sum_{h=1}^{\infty} A_N(p^h)\right)$$

BEWEIS
Dies folgt sofort aus der Multiplikativität von A_N und der absoluten Konvergenz der Reihe. □

DEFINITION 3.7.2
Wir setzen

$$\chi_N(p) \;=\; 1+\sum_{h=1}^{\infty} A_N(p^h) \;\;,\;\; M_{N,s}(q) \;=\; \left|\left\{(x_1,\ldots,x_s)\in \mathbb{Z}/q\mathbb{Z} \mid x_1^k+\cdots+x_s^k \equiv N \bmod q\right\}\right|$$

und schreiben kurz $M_N(q) = M_{N,s}(q)$.

LEMMA 3.7.6
Es ist

$$\chi_N(p) \;=\; \lim_{h\to\infty} \frac{M_{N,s}(p^h)}{p^{h\cdot(s-1)}}\,.$$

BEWEIS
Ist $d = \mathrm{ggT}(a,q)$, dann gilt

$$S(a,q) \;=\; \sum_{x=1}^{q} e\left(\tfrac{ax^k}{q}\right) \;=\; \sum_{x=1}^{q} e\left(\tfrac{\frac{a}{d}\cdot x^k}{\frac{q}{d}}\right) \;=\; d\cdot \sum_{x=1}^{\frac{q}{d}} e\left(\tfrac{\frac{a}{d}\cdot x^k}{\frac{q}{d}}\right) \;=\; d\cdot S(\tfrac{q}{d},\tfrac{a}{d})\,. \tag{1}$$

Aus

$$\frac{1}{q}\sum_{a=1}^{q} e\left(\tfrac{am}{q}\right) \;=\; \begin{cases} 1 & \text{falls} \quad m\equiv 0 \bmod q \\ 0 & \text{falls} \quad m\not\equiv 0 \bmod q \end{cases}$$

folgt

$$\frac{1}{q}\sum_{a=1}^{q} e\left(\tfrac{a(x_1^k+\cdots+x_s^k-N)}{q}\right) \;=\; \begin{cases} 1 & \text{falls} \quad x_1^k+\cdots+x_s^k\equiv N \bmod q \\ 0 & \text{falls} \quad x_1^k+\cdots+x_s^k\not\equiv N \bmod q \end{cases}$$

und damit

$$M_N(q) \;=\; \sum_{x_1=1}^{q}\cdots\sum_{x_s=1}^{q}\frac{1}{q}\sum_{a=1}^{q} e_q(a(x_1^k+\cdots+x_s^k-N)) \;=\; \frac{1}{q}\sum_{a=1}^{q}\sum_{x_1=1}^{q}\cdots\sum_{x_s=1}^{q} e_q(a(x_1^k+\cdots+x_s^k-N))$$

$$=\; \frac{1}{q}\sum_{a=1}^{q}\sum_{x_1=1}^{q} e_q(ax_1^k)\;\cdots\sum_{x_s=1}^{q} e_q(ax_s^k)e_q(-Na) \;=\; \frac{1}{q}\sum_{a=1}^{q} S(a,q)^s\cdot e_q(-Na)$$

$$=\; \frac{1}{q}\sum_{d|q}\sum_{\substack{a=1\\(a,q)=d}}^{q} S(a,q)^s\cdot e(-Na) \;\underset{(1)}{=}\; \frac{1}{q}\sum_{d|q}\sum_{\substack{a=1\\(a,q)=d}}^{q} d^s\cdot S(\tfrac{a}{d},\tfrac{q}{d})^s\cdot e_{\frac{q}{d}}(-N\tfrac{a}{d})$$

$$=\; \frac{1}{q}\sum_{d|q}\sum_{\substack{a=1\\(a,q)=d}}^{q} q^s\left(\tfrac{S(\frac{a}{d},\frac{q}{d})}{\frac{q}{d}}\right)^s\cdot e_{\frac{q}{d}}(-N\tfrac{a}{d}) \;=\; q^{s-1}\sum_{d|q} A_N(\tfrac{q}{d})\,.$$

Also ist

$$\sum_{d|q} A_N(\tfrac{q}{d}) \;=\; q^{1-s}\cdot M_N(q)$$

für alle $q \geq 1$. Speziell für $q = p^h$ folgt

$$1 + \sum_{j=1}^{h} A_N(p^j) \;=\; \sum_{d|p^h} A_N(\tfrac{p^h}{d}) \;=\; p^{h(1-s)} \cdot M_N(p^h)$$

und somit

$$\chi_N(p) \;=\; \lim_{h\to\infty} \left(1 + \sum_{j=1}^{h} A_N(p^j) \right) \;=\; \lim_{h\to\infty} \left(p^{h(1-s)} \cdot M_N(p^h) \right) .$$

Der Grenzwert ist endlich, weil die A_N asymptotisch durch $\frac{1}{q^{1+\delta_4}}$ beschränkt sind. □

Es bleibt noch $\chi_N(p) > 0$ zu zeigen. Wir beginnen mit einer Tatsache aus der Theorie der k-ten Potenzreste.

Definition 3.7.3
Es sei $q \in \mathbb{N}$. Ein $N \in \mathbb{Z}$ mit $\mathrm{ggT}(N, q) = 1$ bzw. die Restklasse $N \bmod q$ heißt <u>k-ter Potenzrest</u>, falls die Kongruenz

$$(*) \qquad x^k \;\equiv\; N \mod q$$

lösbar ist.

Lemma 3.7.7
Es sei $k \geq 2$ und $p > 2$ eine Primzahl. Dann gibt es mindestens $\frac{p-1}{k}$ k-te Potenzreste mod p (wenn nur paarweise verschiedene Restklassen gezählt werden).

Beweis
Da $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist (Satz 0.0.10), hat die Kongruenz $x^k \equiv a \bmod p$ höchstens k Lösungen mod p. Die Potenzen $1^k, 2^k, \ldots, (p-1)^k$ gehören daher mindestens $\frac{p-1}{k}$ verschiedenen Restklassen mod p an. □

Lemma 3.7.8
Es sei $p > 2$ eine Primzahl und $N \in \mathbb{Z}$ mit $p \nmid N$. Dann ist $M_{N,s}(p) > 0$ für $s \geq 2k - 1$.

Beweis
Für $N \in \mathbb{Z}$ sei $s(N)$ das kleinste $s \in \mathbb{N}$ für welches die Kongruenz

$$(1) \qquad x_1^k + \cdots + x_s^k \;\equiv\; N \mod p$$

lösbar ist. Es sei $C(j)$ die Menge aller Restklassen $N \bmod p$, so dass $\mathrm{ggT}(N, p) = 1$ und $s(N) = j$ ist. Aus (1) folgt

$$(mx_1)^k + \cdots + (mx_s)^k \;\equiv\; Nm^k \mod p\,.$$

Daher

$$N \bmod p \;\in\; C(j) \;\;\Leftrightarrow\;\; (Nm^k) \bmod p \;\in\; C(j)\,.$$

Wegen Lemma 3.7.7 folgt

$$(2) \qquad C(j) \neq \emptyset \;\;\Rightarrow\;\; |C(j)| \geq \frac{p-1}{k}\,.$$

Es sei n die größte natürliche Zahl mit $C(n) \neq \emptyset$. Es ist $1 \in C(1)$ und daher $n \geq 1$. Es sei $2 \leq j < n$ und N die kleinste natürliche Zahl mit $\mathrm{ggT}(N, p) = 1$ und $s(N) > j$. Es ist $\mathrm{ggT}(N-1, p) = 1$ oder $\mathrm{ggT}(N-2, p) = 1$, $N - 1 \in \mathbb{N}$ oder $N - 2 \in \mathbb{N}$. Dann ist $s(N-1) \leq j$ oder $s(N-2) \leq j$. Wegen $N = (N-1) + 1^k$ und $N = (N-2) + 1^k + 1^k$ folgt, dass

$$j + 1 \;\leq\; s(N) \;\leq\; s(N-i) + 2 \;\leq\; j + 2$$

für $i = 1, 2$ ist. Damit sind für keine zwei aufeinander folgenden Werte von j die Mengen $C(j)$ leer, und daher ist die Anzahl der nichtleeren Mengen $C(j)$ mindestens $\frac{n+1}{2}$. Da die $C(j)$ paarweise disjunkt sind, folgt mit (2)

$$p - 1 \;=\; \sum_{\substack{j=1 \\ C(j)\neq\emptyset}}^{n} |C(j)| \;\geq\; \frac{n+1}{2} \cdot \frac{p-1}{k}$$

und damit $n \leq 2k - 1$. □

Definition 3.7.4
Es sei $k \geq 2$ und p eine Primzahl. Dann setzen wir $k = p^\tau \cdot k_0$ mit $\mathrm{ggT}(k_0, p) = 1$, sowie

$$\gamma \;=\; \gamma(p,k) \;=\; \begin{cases} 2\tau + 1 & \text{falls} \quad p = 2 \\ \max(1, 2\tau) & \text{falls} \quad p > 2 \end{cases} .$$

Lemma 3.7.9
Es sei $\mathrm{ggT}(N, p) = 1$ *und* $h \geq \gamma(p,k)$*. Ist die Kongruenz*

$$y^k \;\equiv\; N \mod p^h$$

lösbar, so auch die Kongruenz

$$y^k \;\equiv\; N \mod p^{h+1} .$$

Beweis
Es sei $y_h^k \equiv N \bmod p^h$. Wir setzen für $t \in \mathbb{Z}$: $y = y_h + tp^{h-\tau}$. Dann ist

$$(1) \qquad (y_h + tp^{h-\tau})^k \;=\; y_h^k + k_0 y_h^{k-1} tp^h \;+\; \binom{k}{2} y_h^{k-2} t^2 p^{2(h-\tau)} \;+\; \cdots .$$

Im Fall $p > 2$ haben wir

$$p^{2h-\tau} \mid \binom{k}{2} y_h^{k-2} t^2 p^{2(h-\tau)} \;\text{ und }\; p^{3(h-\tau)} \mid \binom{k}{l} y_h^{k-l} t^l p^{l(h-\tau)} \text{ für } l \geq 3 .$$

Im Fall $p = 2$ haben wir

$$p^{2(h-\tau)} \mid \binom{k}{l} y_h^{k-l} t^l p^{l(h-\tau)} .$$

Wegen $h \geq \gamma$ folgt aus (1) stets

$$y^k \;\equiv\; y_h^k \;+\; k_0 y_h^{k-1} tp^h \mod p^{h+1} .$$

Die Kongruenz

$$k_0 y_h^{k-1} t \;\equiv\; \frac{N - y_h^k}{p^h} \mod p$$

besitzt eine Lösung $t = t_h$. Die Wahl $y_{h+1} = y_h + t_h p^{h-\tau}$ erfüllt daher die gesuchte Kongruenz

$$y_{h+1}^k \;\equiv\; N \mod p^{h+1} .$$

□

Lemma 3.7.10
Es sei p *eine Primzahl und* $N \in \mathbb{Z}$*. Wenn es* $a_1, \ldots, a_s \in \mathbb{Z}$ *gibt, die nicht alle durch* p *teilbar sind, so dass*

$$(1) \qquad a_1^k + \cdots + a_s^k \;\equiv\; N \mod p^\gamma$$

gilt, dann ist $M_{N,s}(p^h) \geq p^{(h-\gamma)\cdot(s-1)}$ *für* $h \geq \gamma$.

Beweis
Es sei ohne Einschränkung $\mathrm{ggT}(a_1, p) = 1$. Der Fall $h = \gamma$ ist klar, es sei also $h > \gamma$. Dann gibt es $p^{(h-\gamma)(s-1)}$ $(s-1)$-Tupel

$$\vec{x}_h \;=\; (x_{2,h} \bmod p^h, \ldots, x_{s,h} \bmod p^h)$$

mit $x_{i,h} \equiv a_i \bmod p^\gamma$. Da die Kongruenz

$$x_{1,\gamma}^k \;\equiv\; N - x_{2,h}^k - \cdots - x_{s,h}^k \mod p^\gamma$$

für jedes $\vec{x}_h$ durch $x_{1,\gamma} = a_1 \not\equiv 0 \bmod p$ gelöst wird, gibt es nach Lemma 3.7.9 zu jedem $\vec{x}_h$ eine Lösung von

$$x_1^k + \cdots + x_s^k \;\equiv\; N \mod p^h$$

mit $x_i = x_{i,h}$ für $2 \le i \le s$. Daraus folgt die Behauptung. □

Lemma 3.7.11
Es sei $s \ge 2^k + 1$, $N \in \mathbb{Z}$ und p eine Primzahl. Dann ist die Kongruenz

$$(*) \qquad x_1^k + \cdots + x_s^k \;\equiv\; N \mod p^\gamma$$

lösbar.

Beweis
Es sei zunächst $\tau = 0$. Dann ist $\gamma = 1$ und die Behauptung folgt aus Lemma 3.7.8 wegen $2^k + 1 \ge 2k - 1$ für $k \ge 2$. Es sei nun $\tau > 0$ und $p > 2$. Dann folgt wegen $k = p^\tau k_0$ und $\gamma = 2\tau$: $k^2 \ge p^\gamma$. Wegen $s \ge 2^k + 1 \ge k^2 \ge p^\gamma$ ist die Kongruenz $(*)$ mit $x_j \in \{0, 1\}$ lösbar. Für $\tau > 0$ und $p = 2$ ist $k^2 \ge p^\gamma$. Es ist $s \ge 2^k + 1 \ge k^3$ für $k \ge 10$, und die Kongruenz $(*)$ ist mit $x_j \in \{0, 1\}$ lösbar. In den verbleibenden Fällen $p = 2$ und $k = 2, 4, 6, 8$ wird die Behauptung leicht durch Nachrechnen gezeigt. □

Lemma 3.7.12
Es sei $s \ge 2^k + 1$. Dann ist $\chi_N(p) > 0$ für alle $N \in \mathbb{Z}$ und für alle Primzahlen p.

Beweis
Dies folgt aus den Lemmata 3.7.6, 3.7.10 und 3.7.11. □

Lemma 3.7.13
Es sei $s \ge 2^k + 1$. Dann gibt es Konstanten $c_1 = c_1(k, s) > 0$ und $c_2 = c_2(k, s) > 0$, so dass

$$c_1 \;<\; \mathfrak{S}(N) \;<\; c_2$$

gilt.

Beweis
Die Abschätzung von oben folgt aus Lemma 3.7.2, die Abschätzung von unten aus der Produktdarstellung von 3.7.5 und der Positivität der Faktoren (Lemma 3.7.12). □

Jetzt haben wir alle Bestandteile für den

Beweis von Satz 3.2.1
Es ist

$$r_{k,s}(N) \;=\; \int\limits_{\mathcal{M}_1} F(\alpha)^s e(-N\alpha) d\alpha \;+\; \int\limits_{\mathcal{M}_2} F(\alpha)^s e(-N\alpha) d\alpha \,.$$

Nach Lemma 3.5.3 ist

$$\int\limits_{\mathcal{M}_1} F(\alpha)^s e(-N\alpha) d\alpha \;=\; \mathfrak{S}(N, P^\nu) J^*(N) \;+\; O\left(P^{s-k-\delta_2}\right) .$$

Nach Satz 3.6.1 und Satz 3.6.3 ist

$$J^*(N) \;=\; \Gamma\left(1 + \tfrac{1}{k}\right)^s \cdot \Gamma\left(\tfrac{s}{k}\right)^{-1} \cdot N^{\frac{s}{k}-1} \;+\; O\left(P^{s-k-\delta_3}\right) .$$

Nach Lemma 3.7.2 ist

$$\mathfrak{S}(N) \; - \; \mathfrak{S}(N, P^\nu) \; \ll \; P^{-\nu\delta_4} \, .$$

Also gibt es $\delta > 0$, so dass

$$\int\limits_{\mathcal{M}_1} F(\alpha)^s e(-N\alpha) d\alpha \; = \; \mathfrak{S}(N) \cdot \Gamma\left(1 + \tfrac{1}{k}\right)^s \cdot \Gamma\left(\tfrac{s}{k}\right)^{-1} \cdot N^{\frac{s}{k}-1} \; + \; O_{k,s}\left(N^{\frac{s}{k}-1-\delta}\right)$$

gilt. Satz 3.2.1 folgt nun aus Satz 3.4.1 und Lemma 3.7.13. □

3.8. Ausblick

Wir haben in dieser Vorlesung Anwendungen von Abschätzungen von Weylschen Exponentialsummen kennengelernt. Eine der wichtigsten Folgerungen war ein Resultat über die nullstellenfreie Zone der ζ-Funktion (Satz 1.10.6):

$$\zeta(s) \; \neq \; 0 \quad \text{für} \quad t \geq 0 \text{ und}$$

$$\sigma \; \geq \; 1 - A_0 \cdot \frac{\log(\log(t))}{\log(t)} \, . \tag{1}$$

Eine Anwendung dieses Resultats war die Existenz von Primzahlen in kurzen Intervallen: es gibt $\delta > 0$, so dass

$$\lim_{x \to \infty} \frac{\psi(x) - \psi(x - x^{1-\delta})}{x^{1-\delta}} \; = \; 1 \, .$$

Wir haben ferner gesehen, dass $\delta > 0$ durch $1 - b^{-1} + \varepsilon$ mit $\varepsilon > 0$ ersetzt werden kann, falls eine Nullstellendichteabschätzung der Form

$$N(\sigma, T) \; \ll \; T^{b(1-\sigma)+\varepsilon} \cdot (\log T)^c$$

gilt, und A_0 in (1) durch $A_0(t) \to \infty$ für $t \to \infty$ ersetzt werden kann. Eine solche Verbesserung von (1) kann nun durch die Exponentialsummenmethode von Vinogradoff erreicht werden:

$$\zeta(s) \; \neq \; 0 \quad \text{für} \quad t \geq 0 \text{ und}$$

$$\sigma \; \geq \; 1 - (\log(t))^{-\frac{2}{3}+\varepsilon} \, . \tag{2}$$

Diese Abschätzung ergibt auch das schärfste bis heute bekannte Restglied im Primzahlsatz:

$$\pi(x) \; = \; \mathrm{li}(x) \; + \; O\left(x \cdot \exp\left(-\log(x)^{\frac{3}{5}-\varepsilon}\right)\right) \, .$$

Auch im Waringschen Problem ergibt die Vinogradoffsche Methode Verbesserungen: $G(k) \leq 2^k + 1$ kann zu $G(k) \ll k \cdot \log(k)$ verbessert werden.

Index