SATZ 1: *Sei* $f: \mathbb{N} \to \mathbb{C}$ *eine multiplikative Funktion, und sei die Reihe*

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

absolut konvergent. Dann ist $F(s)$ *gleich dem Euler-Produkt*

$$(8) \qquad F(s) = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \ldots\right) ,$$

wo das Produkt über alle Primzahlen p *läuft und auch absolut konvergiert.*

Beispiele: c) Für $\zeta(s)$ sind die Koeffizienten alle gleich 1, also

$$(9) \qquad \zeta(s) = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots\right) = \prod_p \frac{1}{1-p^{-s}} \qquad (\sigma > 1) .$$

Diese von Euler entdeckte Produktentwicklung ist der Grund für die große Rolle, die die Zetafunktion in der Primzahltheorie spielt. Außerdem lehrt sie, daß für $\sigma > 1$ die Funktion $\zeta(s)$ nie verschwinden kann (da das Produkt konvergent ist und seine einzelnen Glieder nicht Null sind). Für die in a) und b) angegebenen Reihen erhält man

$$\sum_{n=1}^{\infty} \frac{d(n)}{n^s} = \zeta(s)^2 = \prod_p (1 - p^{-s})^{-2}$$

$$= \prod_p (1 + 2p^{-s} + 3p^{-2s} + \ldots)$$

$$= \prod_p \left(1 + \frac{d(p)}{p^s} + \frac{d(p^2)}{p^{2s}} + \ldots\right) ,$$

$$\sum_{n=1}^{\infty} \frac{\sigma_k(n)}{n^s} = \zeta(s)\,\zeta(s-k) = \prod_p [(1 - p^{-s})(1 - p^{k-s})]^{-1}$$

$$= \prod_p \left(1 + \frac{p^{k+1}}{p^s} + \frac{p^{2k}+p^k+1}{p^{2s}} + \ldots\right)$$

$$= \prod_p \left(1 + \frac{\sigma_k(p)}{p^s} + \frac{\sigma_k(p^2)}{p^{2s}} + \ldots\right) ,$$

also sind die beiden Funktionen $n \mapsto d(n)$ und $n \mapsto \sigma_k(n)$ multiplikativ (was man auch direkt leicht sieht), da trivialerweise die Umkehrung von Satz 1 gilt: besitzt eine Dirichletsche Reihe ein Euler-Produkt (8), so stellen die Koeffizienten dieser Reihe eine multiplikative Funktion dar.

d) Für den Kehrwert $\frac{1}{\zeta(s)}$ erhalten wir

$$(10) \qquad \frac{1}{\zeta(s)} = \prod_p (1 - p^{-s}) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} ,$$

wo $\mu(n)$ die multiplikative Funktion ist, die für Primzahlpotenzen die Werte $\mu(p) = -1$, $\mu(p^r) = 0$ $(r \geq 2)$ annimmt, d.h.

$$(11) \qquad \mu(n) = \begin{cases} 0, \text{ falls } n \text{ ein Quadrat enthält} \\ (-1)^k, \text{ falls } n = p_1 \cdots p_k,\ p_1 < \ldots < p_k \end{cases}$$

Die Funktion $\mu(n)$ ist die sogenannte *Möbiussche Funktion*. Aus der Beziehung $\zeta(s) \cdot \frac{1}{\zeta(s)} = 1$ und der Faltungsformel (3) folgt die wichtige Eigenschaft dieser Funktion, daß

$$(12) \qquad \sum_{d|n} \mu(d) = \begin{cases} 1, \text{ falls } n = 1 \\ 0, \text{ falls } n > 1 . \end{cases}$$

Die Möbiussche Funktion ist wegen folgender *Möbiusschen Umkehrformel* wichtig.

SATZ 2: *Seien* f *und* g *zwei Funktionen von* $\mathbb{N}$ *nach* $\mathbb{C}$. *Ist für alle* n

$$(13) \qquad f(n) = \sum_{d|n} g(d) ,$$

so ist für alle n

$$(14) \qquad g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d)$$

und umgekehrt. Stehen f *und* g *in dieser Beziehung zueinander, so ist* g *multiplikativ genau dann, wenn* f *multiplikativ ist.*

Beweis: Die erste Aussage ist leicht aus (12) herzuleiten; wir wollen sie aber durch Anwendung von Dirichletschen Reihen erhalten, um Übung im Umgang mit solchen Reihen zu bekommen. Die Gleichungen

$$\begin{aligned} f(1) &= g(1) \\ f(2) &= g(1) + g(2) , \\ f(3) &= g(1) + g(3) , \\ f(4) &= g(1) + g(2) + g(4) , \ \ldots \end{aligned}$$

lassen sich induktiv für g lösen:

$$\begin{aligned} g(1) &= f(1) , \\ g(2) &= f(2) - f(1) , \\ g(3) &= f(3) - f(1) , \\ g(4) &= f(4) - f(2) , \ \ldots \end{aligned}$$

Es ist also klar, daß eine Beziehung wie (14) mit von f unabhängigen Koeffizienten existieren muß; somit brauchen wir (13) $\leftrightarrow$ (14) nur für Folgen $\{f(n)\}$, $\{g(n)\}$ von langsamem Wachstum zu beweisen (z.B. nur für solche mit $g(n) = 0$ für $n > n_0$) und können deshalb annehmen, daß die zugehörigen Dirichletschen Reihen

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} , \quad G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}$$

absolut konvergent sind (für mindestens ein s). Dann gilt wegen der Faltungsformel (3) und der Beziehung (10)

$$(13) \leftrightarrow F(s) = \sum_{n=1}^{\infty} 1.n^{-s} \sum_{m=1}^{\infty} g(m)m^{-s} = \zeta(s)\, G(s)$$

$$\leftrightarrow G(s) = \zeta(s)^{-1} F(s) = \sum_{n=1}^{\infty} \mu(n)n^{-s} \sum_{m=1}^{\infty} f(m)m^{-s}$$

$$\leftrightarrow (14) ,$$

und, wenn (13) und (14) gelten,

g multiplikativ $\leftrightarrow$ $G(s)$ besitzt eine Eulersche Produktentwicklung

$\leftrightarrow$ $F(s) = \zeta(s)\, G(s)$ besitzt eine Eulersche Produktentwicklung

$\leftrightarrow$ f multiplikativ .

<u>Beispiel</u>: Sei $\nu(n)$ die Anzahl der Primteiler von n (mit Multiplizität: $\nu(p_1^{r_1}\ldots p_k^{r_k}) = r_1 + \ldots + r_k$) und $\lambda(n) = (-1)^{\nu(n)}$. Dann ist $\lambda(n)$ multiplikativ und

$$(15) \qquad \sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s} = \prod_p \left[1 - \frac{1}{p^s} + \frac{1}{p^{2s}} - \ldots\right] = \prod_p \left(\frac{1}{1+p^{-s}}\right)$$

$$= \prod_p \left(\frac{1-p^{-s}}{1-p^{-2s}}\right) = \frac{\zeta(2s)}{\zeta(s)} \qquad (\sigma > 1) ,$$

also gilt (14) mit $g = \lambda$ und

$$f(n) = \text{Koeffizient von } n^{-s} \text{ in } \zeta(2s)$$

$$(16) \qquad = \begin{cases} 1, \text{ falls } n \text{ eine Quadratzahl ist,} \\ 0 \text{ sonst .} \end{cases}$$

Es gilt also

$$(17) \qquad f(n) = \sum_{d|n} \lambda(d) .$$

3. Man beweise für $\sigma > 1$ die Beziehung

$$\zeta(s) = \frac{s}{s-1} - \frac{s}{2!}[\zeta(s+1) - 1] - \frac{s(s+1)}{3!}[\zeta(s+2) - 1] - \dots ,$$

indem man $\zeta(s) = \sum n^{-s}$ einsetzt und die Summationen vertauscht; man benutze diese Formel, um zu zeigen, daß $\zeta(s) - \frac{s}{s-1}$ sich holomorph in ganz $\mathbb{C}$ fortsetzen läßt.

4. Man zeige, daß

$$(17) \qquad \zeta(s) = \frac{1}{s-1} + \gamma + O(s-1) \qquad (s \to 1)$$

gilt, wo γ die Eulersche Konstante ist.

§5 Charaktere

Die wichtigsten Dirichletschen Reihen (neben der Zetafunktion) sind die "L-Reihen", die ebenfalls von Dirichlet eingeführt wurden und von ihm benutzt wurden, um

a) die Existenz unendlich vieler Primzahlen in jeder arithmetischen Folge $\{Nk+a\}_{k\in\mathbb{Z}}$ mit $(N,a) = 1$ zu beweisen, und

b) eine Formel anzugeben für die Anzahl der Äquivalenzklassen von binären quadratischen Formen mit gegebener Diskriminante.

Die L-Reihen sind Funktionen, die gewissen Charakteren zugeordnet sind, und bevor wir in §§ 6 - 8 eine Beschreibung von Dirichlets Ergebnissen geben können, müssen wir diese Charaktere etwas studieren.

Ein *Charakter* auf einer endlichen Gruppe G ist ein Homomorphismus

$$\chi : G \to \mathbb{C}^* ,$$

wo $\mathbb{C}^*$ die Gruppe der von Null verschiedenen komplexen Zahlen ist (mit der Multiplikation als Gruppenoperation). Falls χ und χ' zwei Charaktere auf G sind, können wir das *Produkt* $\chi\chi'$ und das *Inverse* χ^{-1} durch

$$\chi\chi'(g) = \chi(g)\,\chi'(g) , \quad \chi^{-1}(g) = \chi(g)^{-1} \qquad (\forall g \in G)$$

definieren. Somit bilden die Charaktere auf G eine Gruppe, die wir mit $\hat{G}$ bezeichnen.

SATZ 1: *Sei* G *eine endliche abelsche Gruppe. Dann ist* $\hat{G}$ *zu* G *isomorph. Insbesondere ist* $|\hat{G}| = |G|$.

Beweis: Bekanntlich ist G eine direkte Summe von endlichen zyklischen Gruppen, also hat G Erzeugende $g_1, \ldots, g_k$ der Ordnungen $n_1, \ldots, n_k$ und jedes Element $g \in G$ läßt sich in der Gestalt $g = g_1^{r_1} \ldots g_k^{r_k}$ schreiben mit $r_1, \ldots, r_k \in \mathbb{Z}$. Ist χ ein Charakter auf G und $\chi(g_i) = \xi_i$ $(i = 1, \ldots, k)$, so ist

$$\xi_i^{n_i} = \chi(g_i)^{n_i} = \chi(g_i^{n_i}) = \chi(e) = 1$$

und

$$\chi(g_1^{r_1} \ldots g_k^{r_k}) = \chi(g_1)^{r_1} \ldots \chi(g_k)^{r_k} = \xi_1^{r_1} \ldots \xi_k^{r_k} , \tag{1}$$

d.h. die ξ_i sind n_i-te Einheitswurzeln und χ ist durch die ξ_i bestimmt. Umgekehrt, wenn $\xi_1, \ldots, \xi_k \in \mathbb{C}^*$ mit $\xi_i^{n_i} = 1$ $(i = 1, \ldots, k)$ beliebig gewählt werden, so definiert (1) einen Charakter. Es gibt also eine bijektive Korrespondenz zwischen Charakteren χ und k-Tupeln $(\xi_1, \ldots, \xi_k)$ mit $\xi_i^{n_i} = 1$, wobei das Produkt von Charakteren dem Produkt der ξ_i entspricht. Somit ist

$$\hat{G} \cong \{(\xi_1, \ldots, \xi_k) \in \mathbb{C}^k \mid \xi_1^{n_1} = \ldots = \xi_k^{n_k} = 1\}$$

$$\cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z} \cong G .$$

Bemerkung: Für G endlich ist $\chi(g)$ für jedes $g \in G$ eine Einheitswurzel, also vom Absolutbetrag 1, und somit ist der durch

$$\bar{\chi}(g) = \overline{\chi(g)} \qquad (\forall g \in G)$$

erklärte zu χ konjugierte Charakter mit dem oben definierten inversen Charakter identisch.

Definition: Ein *Dirichletscher Charakter modulo* N (N eine natürliche Zahl) ist ein Charakter auf der Gruppe

$$(\mathbb{Z}/N\mathbb{Z})^\times = \{n \pmod N \mid (n,N) = 1\} .$$

Wenn χ ein solcher Charakter ist, definieren wir eine (ebenfalls mit χ bezeichnete) Funktion $\chi: \mathbb{Z} \to \mathbb{C}$ durch

$$\chi(n) = \begin{cases} \chi(n \pmod N) , & \text{falls } (n,N) = 1 \\ 0 , & \text{falls } (n,N) > 1 . \end{cases}$$

Auch diese Funktion χ wird als Dirichletscher Charakter bezeichnet.

Ein Dirichletscher Charakter (mod N) kann auch beschrieben werden als eine Funktion $\chi: \mathbb{Z} \to \mathbb{C}$ mit den Eigenschaften

(1) $\chi(n) = 0 \iff (n,N) > 1$

(2) χ ist streng multiplikativ: $\chi(mn) = \chi(m)\,\chi(n)$ für alle $m,n \in \mathbb{Z}$

(3) $\chi(n)$ hängt nur von n (mod N) ab.

Nach Satz 1 gibt es $\phi(N)$ Dirichletsche Charaktere, wo

$$\phi(N) = |(\mathbb{Z}/N\mathbb{Z})^{\times}| = \#\{n \pmod N \mid (n,N) = 1\}$$

$$= N \prod_{p \mid N} \left(1 - \frac{1}{p}\right)$$

die Eulersche Funktion von N bezeichnet.

Beispiele: a) Für jedes N ist der *Hauptcharakter* χ_0 (mod N) durch

$$\chi_0(n) = \begin{cases} 1 & (n,N) = 1 \\ 0 & (n,N) > 1 \end{cases}$$

erklärt (das entspricht der Eins von $\widehat{(\mathbb{Z}/N\mathbb{Z})^{\times}}$).

b) Für $N = 2$ ist $\phi(N) = 1$, also χ_0 der einzige Charakter. Für $N = 3, 4, 6$ ist $\phi(N)$ jeweils gleich 2, und es gibt neben dem Hauptcharakter die Charaktere

n	0	1	2	3	4	5	6	...
$\varepsilon_3(n)$	0	1	-1	0	1	-1	0	...

n	0	1	2	3	4	5	6	7	8	...
$\varepsilon_4(n)$	0	1	0	-1	0	1	0	-1	0	...

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	...
$\varepsilon_6(n)$	0	1	0	0	0	-1	0	1	0	0	0	-1	0	1	...

Für $N = 5$ gibt es neben χ_0 drei Charaktere:

n (mod 5)	0	1	2	3	4
$\chi(n)$	0	1	i	-i	-1
	0	1	-1	-1	1
	0	1	-i	+i	-1

c) Für jede Primzahl p ist das *Legendresche Symbol*

$$(2) \qquad \left(\frac{n}{p}\right) = \begin{cases} 0, & \text{falls } p \mid n \\ 1, & \text{falls } p \nmid n,\ n \equiv x^2 \pmod p \text{ für ein } x \in \mathbb{Z} \\ -1, & \text{sonst} \end{cases}$$

ein Dirichletscher Charakter (mod p).

Wir haben zwei einfache, aber sehr nützliche Sätze:

SATZ 2: *Sei* χ *ein Dirichletscher Charakter modulo* N. *Dann ist*

$$(3) \qquad \sum_{n \pmod N} \chi(n) = \begin{cases} \phi(N), & \text{falls } \chi = \chi_0 \\ 0, & \text{falls } \chi \neq \chi_0 . \end{cases}$$

(Hier bezeichnet $\sum_{n \pmod N}$ eine Summe über ein beliebiges Vertretersystem von $\mathbb{Z}/N\mathbb{Z}$, z.B. $\sum_{n=1}^{N}$.)

KOROLLAR: *Seien* χ_1, χ_2 *zwei Dirichletsche Charaktere* (mod N). *Dann ist*

$$(4) \qquad \frac{1}{\phi(N)} \sum_{n \pmod N} \chi_1(n)\, \bar{\chi}_2(n) = \begin{cases} 1, & \text{falls } \chi_1 = \chi_2 \\ 0, & \text{falls } \chi_1 \neq \chi_2 . \end{cases}$$

Beweis: Für $\chi = \chi_0$ ist (3) trivial. Sei $\chi \neq \chi_0$ und $m \in \mathbb{Z}$ so gewählt, daß $(m,N) = 1$ und $\chi(m) \neq 1$ ist. Dann ist

$$(1 - \chi(m)) \sum_{n \pmod N} \chi(n) = \sum_{n \pmod N} [\chi(n) - \chi(mn)]$$

$$= \sum_{n \pmod N} \chi(n) - \sum_{n \pmod N} \chi(n) = 0$$

(da mit n auch mn ein Vertretersystem von $\mathbb{Z}$ (mod N) durchläuft), also, da $\chi(m) \neq 1$,

$$\sum_{n \pmod N} \chi(n) = 0 .$$

Das Korollar folgt, indem man $\chi_1 \bar{\chi}_2$ für χ wählt.

SATZ 3: *Sei* $n \in \mathbb{Z}$. *Dann ist*

$$(5) \qquad \sum_{\chi} \chi(n) = \begin{cases} \phi(N), & \text{falls } n \equiv 1 \pmod N \\ 0, & \text{falls } n \not\equiv 1 \pmod N , \end{cases}$$

wobei über alle Dirichletschen Charaktere (mod N) *summiert wird.*

Korollar: *Seien* $a,b \in \mathbb{Z}$, $(b,N) = 1$. *Dann ist*

$$(6) \qquad \frac{1}{\phi(N)} \sum_{\chi} \chi(a)\,\bar{\chi}(b) = \begin{cases} 1, & \textit{falls } a \equiv b \pmod N \\ 0, & \textit{falls } a \not\equiv b \pmod N \end{cases}.$$

Beweis: Für $n \equiv 1 \pmod N$ ist (5) trivial, da es $\phi(N)$ Charaktere gibt und für alle χ $\chi(n) = 1$ gilt. Für $(n,N) > 1$ gilt (5) auch, da dann $\chi(n)$ für alle χ verschwindet. Sei $n \not\equiv 1 \pmod N$, $(n,N) = 1$, und χ_1 ein Dirichletscher Charakter (mod N) mit $\chi_1(n) \neq 1$. Ein solcher existiert wegen Satz 1, denn die Charaktere χ mit $\chi(n) = 1$ sind Charaktere auf der Quotientengruppe $(\mathbb{Z}/N\mathbb{Z})^\times/\langle n\rangle$, und deren Anzahl ist demnach kleiner als $|(\mathbb{Z}/N\mathbb{Z})^\times|$. Dann ist

$$\begin{aligned}(1 - \chi_1(n)) \sum_{\chi} \chi(n) &= \sum_{\chi} [\chi(n) - \chi\chi_1(n)] \\ &= \sum_{\chi} \chi(n) - \sum_{\chi} \chi(n) = 0\,,\end{aligned}$$

da $\chi\chi_1$ mit χ über die Gruppe $(\mathbb{Z}/N\mathbb{Z})^\times$ läuft. Da $1 - \chi_1(n) \neq 0$, folgt hieraus, daß die Summe verschwindet. Das Korollar folgt, indem man n mit $nb \equiv a \pmod N$ wählt.

Sei N_1 ein von N verschiedener Teiler von N und χ_1 ein Charakter (mod N_1). Dann definiert die Zusammensetzung

$$(7) \qquad (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/N_1\mathbb{Z})^\times \xrightarrow{\chi_1} \mathbb{C}^*\,,$$

wobei der erste Pfeil die Reduktion (mod N_1) ist, einen Charakter χ (mod N). Wir sagen, daß χ von χ_1 *induziert* wird und nennen einen Charakter χ, der so entsteht, *imprimitiv*; ein Charakter, der nicht auf diese Weise erhalten werden kann, heißt *primitiv* (oder *eigentlich*). Z.B. ist der Hauptcharakter χ_0 (mod N) für $N > 1$ nie primitiv, weil er von dem trivialen Charakter (mod 1) induziert wird. Für jeden Dirichletschen Charakter χ (mod N) gibt es eine kleinste Zahl N_1, so daß χ dargestellt werden kann als die Zusammensetzung (7) mit geeignetem Charakter χ_1 (mod N_1), und dies ist die einzige Darstellung (7) von χ, für die χ_1 primitiv ist. Diese Zahl N_1 mit der Eigenschaft, daß χ von einem primitiven Charakter (mod N_1) induziert wird, nennt man den *Führer* von χ.

Wir werden uns vor allem für *reelle* Charaktere ($\chi = \bar{\chi}$) interessieren, d.h. solche, die nur die Werte 1, 0, -1 annehmen. Wir beweisen einen Satz, in dem alle primitiven reellen Charaktere angegeben

werden.

Definition: Eine *Grundzahl* ist eine ganze Zahl D mit

$$D \equiv 1 \pmod 4,\ D \text{ quadratfrei},$$

oder

$$D \equiv 0 \pmod 4,\ \frac{D}{4} \text{ quadratfrei},\ \frac{D}{4} \equiv 2 \text{ oder } 3 \pmod 4 .$$

(Solche Zahlen nennt man auch *Fundamentaldiskriminanten*). Für eine Grundzahl D definieren wir eine Funktion $\chi_D\colon \mathbb{N} \to \mathbb{Z}$ durch

$$\chi_D(p) = \left(\frac{D}{p}\right) \qquad (p \text{ ungerade Primzahl}) \tag{8a}$$

$$\chi_D(2) = \begin{cases} 0, & \text{falls } D \equiv 0 \pmod 4, \\ 1, & \text{falls } D \equiv 1 \pmod 8, \\ -1, & \text{falls } D \equiv 5 \pmod 8, \end{cases} \tag{8b}$$

$$\chi_D(p_1^{n_1}\cdots p_k^{n_k}) = \chi_D(p_1)^{n_1}\cdots\chi_D(p_k)^{n_k} . \tag{8c}$$

Insbesondere ist χ_1 der triviale Charakter.

SATZ 4: *Die Funktion* $n \mapsto \chi_D(n)$ *(D eine Grundzahl) ist periodisch* (mod $|D|$) *und definiert einen primitiven Dirichletschen Charakter modulo* $|D|$ (ebenfalls mit χ_D bezeichnet) *mit*

$$\chi_D(-1) = \begin{cases} 1, & \textit{falls } D > 0, \\ -1, & \textit{falls } D < 0. \end{cases} \tag{9}$$

Jeder primitive reelle Dirichletsche Charakter ist einer der Charaktere χ_D.

Beweis: Wegen Satz 1 ist jeder Dirichletsche Charakter χ (mod N), mit $N = p_1^{r_1}\cdots p_k^{r_k}$, gleich einem Produkt $\chi_1\cdots\chi_k$, wo χ_i von einem Charakter (mod $p_i^{r_i}$) induziert wird:

$$\begin{array}{ccc} (\mathbb{Z}/N\mathbb{Z})^\times & \xrightarrow{\ \cong\ } & (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times \times\cdots\times (\mathbb{Z}/p_k^{r_k}\mathbb{Z})^\times \\ & {\scriptstyle\chi}\searrow \quad \swarrow{\scriptstyle\chi_1\times\cdots\times\chi_k} & \\ & \mathbb{C}^* & \end{array}$$

Aus dem Diagramm geht hervor, daß χ dann und nur dann primitiv ist, wenn jeder χ_i das ist. Für die Klassifizierung solcher Charaktere genügt es also, sich auf Primzahlpotenzführer $N = p^r$ zu be-

schränken.

Fall i: p ungerade. In diesem Fall ist bekanntlich $(\mathbb{Z}/p^r\mathbb{Z})^\times$ zyklisch (siehe Aufgabe 1). Sei x ein erzeugendes Element ("primitive Wurzel modulo p^r"). Ist χ reell und $\neq \chi_0$, so ist sicherlich $\chi(x) = -1$; es gibt also höchstens einen solchen Charakter. Andererseits ist $n \mapsto (\frac{n}{p})$ ein von χ_0 verschiedener reeller Charakter (mod p^r). Da dieser Charakter den Führer p hat, erhalten wir:

> Für p ungerade gibt es genau einen reellen primitiven Charakter χ (mod p). Dieser ist durch $\chi(n) = (\frac{n}{p})$ gegeben. Es gibt keinen reellen primitiven Charakter modulo p^r mit $r > 1$.

Fall ii: $p = 2$. Für $r = 1$ ist $(\mathbb{Z}/2^r\mathbb{Z})^\times$ trivial, also $\chi = \chi_0$ der einzige Charakter. Für $r = 2$ ist $(\mathbb{Z}/2^r\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$, also ε_4 (Beispiel b) oben) der einzige von χ_0 verschiedene Charakter; er ist auch primitiv. Für $r = 3$ ist $(\mathbb{Z}/2^r\mathbb{Z})^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ und es gibt genau die zwei durch

n (mod 8)	0	1	2	3	4	5	6	7
$\varepsilon_8'(n)$	0	1	0	-1	0	-1	0	1
$\varepsilon_8''(n)$	0	1	0	1	0	-1	0	-1

definierten primitiven reellen Charaktere ε_8' und ε_8'' (es muß $\chi(3) = \alpha$, $\chi(5) = \beta$, $\chi(7) = \chi(3 \times 5) = \alpha\beta$ mit $\alpha, \beta = \pm 1$ sein, und von den 4 Möglichkeiten sind zwei die imprimitiven Charaktere χ_0 und ε_4). Für $r > 3$ ist bekanntlich jede zu 1 (mod 8) kongruente Zahl modulo 2^r zu einem Quadrat kongruent (siehe Aufgabe 1), also gilt für χ reell

$$n \equiv 1 \pmod 8 \Rightarrow n \equiv x^2 \pmod{2^r}$$

$$\Rightarrow \chi(n) = \chi(x^2) = \chi(x)^2 = (\pm 1)^2 = 1 ,$$

und χ kann nicht primitiv sein. Das zeigt:

> Es gibt genau einen primitiven reellen Charakter (ε_4) modulo 4 und genau zwei (ε_8' und ε_8'') modulo 8; für $r \neq 2, 3$ gibt es keinen reellen primitiven Charakter (mod 2^r).

Wir haben jetzt alle reellen primitiven Charaktere gefunden: das sind die Produkte von Legendre Symbolen $(\frac{n}{p})$ für verschiedene ungerade Primzahlen p sowie die Produkte von solchen Charakteren mit ε_4, ε_8' oder ε_8''; insbesondere sind die einzigen Zahlen N, für die

es überhaupt reelle primitive Charaktere gibt, von der Gestalt 1 mal, 4 mal oder 8 mal eine ungerade quadratfreie Zahl. Wir wenden jetzt das quadratische Reziprozitätsgesetz bzw. die sogenannten 1. und 2. Ergänzungssätze an, um folgende Identitäten zu erhalten:

$$\left(\frac{n}{p}\right) = \chi_{p'}(n) \quad \text{für} \quad p \neq 2,\ p \text{ prim, wobei} \quad p' = (-1)^{\frac{p-1}{2}} p \ ,$$

$$\varepsilon_4(n) = \left(\frac{-4}{n}\right) = \chi_{-4}(n) \ ,$$

$$\varepsilon_8'(n) = \left(\frac{8}{n}\right) = \chi_8(n) \ ,$$

$$\varepsilon_8''(n) = \left(\frac{-8}{n}\right) = \chi_{-8}(n) \ .$$

Außerdem ist das Produkt zweier teilerfremder Grundzahlen D_1 und D_2 wieder eine Grundzahl und es gilt

$$\chi_{D_1 D_2} = \chi_{D_1}\chi_{D_2} \qquad ((D_1, D_2) = 1) \ . \tag{10}$$

Somit ist bewiesen, daß die reellen primitiven Charaktere genau die χ_D sind, für die D ein Produkt von teilerfremden Zahlen aus der Menge

$$-4,\ +8,\ -8,\ p\ (p\equiv 1 \pmod 4 \text{ prim}),\ -p\ (p\equiv 3 \pmod 4 \text{ prim}) \tag{11}$$

ist (die Zahlen aus (11) heißen *Primdiskriminanten*). Aber es ist leicht zu sehen, daß jede Grundzahl D ein solches Produkt ist, da D eine der Formen m, $-4m$, $8m$, $-8m$ hat mit m quadratfrei und $m \equiv 1 \pmod 4$, also $m = \prod_{p|m} p'$. Damit sind alle Aussagen des Satzes bewiesen bis auf (9), und auch diese Formel brauchen wir wegen (10) nur für eine Primdiskriminante D zu beweisen, was mit Hilfe des ersten Ergänzungssatzes leicht ist:

$$\chi_{-4}(-1) = \varepsilon_4(-1) = -1 = \operatorname{sign}(-4) \ ,$$

$$\chi_8(-1) = \varepsilon_8'(-1) = 1 = \operatorname{sign}(8) \ ,$$

$$\chi_{-8}(-1) = \varepsilon_8''(-1) = -1 = \operatorname{sign}(-8) \ ,$$

$$\chi_{p'}(-1) = \left(\frac{-1}{p}\right) = \left\{\begin{array}{l} 1, \text{ falls } p \equiv 1 \pmod 4 \\ -1, \text{ falls } p \equiv 3 \pmod 4 \end{array}\right\} = \operatorname{sign}(p') \ .$$

Aufgaben

1. Man beweise die in diesem Paragraphen benutzten Tatsachen

   a) $(\mathbb{Z}/p^r\mathbb{Z})^\times$ ist zyklisch $(p > 2$ prim, $r \geq 1)$,

   b) $n \equiv 1 \pmod 8 \Rightarrow n \equiv x^2 \pmod{2^r}$ $\quad (r \geq 3)$,

   jeweils durch Induktion über r (der Fall $r = 1$ der ersten Aussage ist Spezialfall eines bekannten Satzes über die Einheitengruppe eines endlichen Körpers), indem man das Element, das für p^r eine Lösung liefert, modulo p^{r+1} (bzw. 2^{r-1} für $p = 2$) abändert, um eine Lösung $(\mathrm{mod}\ p^{r+1})$ zu erhalten.

2. Man beweise mit Hilfe von Aufgabe 1 folgende Isomorphismen

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \cong \mathbb{Z}/p^{r-1}(p-1)\mathbb{Z} \qquad (p \text{ ungerade})$$

$$(\mathbb{Z}/2^r\mathbb{Z})^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2^{r-2}\mathbb{Z} \qquad (r \geq 2)$$

   und benutze sie, um *alle* primitiven Dirichletschen Charaktere zu bestimmen. Wieviele gibt es modulo N?

3. Man zeige durch ein Beispiel, daß für einen Dirichletschen Charakter $\chi \pmod N$ der Definitionsmodul (also die Zahl N), die Periode (also die kleinste Zahl r mit $\chi(n+r) = \chi(n)$ für alle n) und der Führer verschieden sein können. Welche Beziehung gibt es zwischen diesen drei Zahlen?

§6 L-Reihen

Sei χ ein Dirichletscher Charakter $(\mathrm{mod}\ N)$. Die χ zugeordnete *Dirichletsche L-Reihe* ist die Reihe

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

Wegen $|\chi(n)| \leq 1$ ist diese Reihe für $\sigma > 1$ absolut konvergent. Wegen der Multiplikativität von χ hat sie nach §2 eine Eulersche Produktdarstellung

$$L(s,\chi) = \prod_p \left(1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \ldots\right) ;$$

wegen der strengen Multiplikativität $\chi(p^r) = \chi(p)^r$ ist sogar

$$L(s,\chi) = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}} \qquad (\sigma > 1) \; . \tag{2}$$

Für den Hauptcharakter χ_0 ist nach (2)

$$\begin{aligned} L(s,\chi_0) &= \prod_p (1 - \chi_0(p)p^{-s})^{-1} \\ &= \prod_{p \nmid N} (1 - p^{-s})^{-1} \\ &= \prod_{p|N} (1 - p^{-s}) \cdot \prod_{\text{alle } p} (1 - p^{-s})^{-1} \\ &= \prod_{p|N} (1 - p^{-s}) \cdot \zeta(s) \; ; \end{aligned} \tag{3}$$

also ist die L-Reihe in diesem Fall bis auf einen einfachen multiplikativen Faktor mit der Riemannschen Zetafunktion identisch. Insbesondere läßt sie sich auf die ganze komplexe Ebene meromorph fortsetzen mit einem einfachen Pol mit Residuum $\prod_{p|N} (1 - p^{-1}) = \frac{\phi(N)}{N}$ an der Stelle $s = 1$ als einziger Singularität.

Für $\chi \neq \chi_0$ ist für $x \to \infty$

$$\begin{aligned} \Big| \sum_{n=1}^{x} \chi(n) \Big| &= \Big| \sum_{n=1}^{N[x/N]} \chi(n) + \sum_{n=N\cdot[\frac{x}{N}]+1}^{x} \chi(n) \Big| \\ &= \Big| [\tfrac{x}{N}] \sum_{n \,(\mathrm{mod}\, N)} \chi(n) + \sum_{n=N[\frac{x}{N}]+1}^{x} \chi(n) \Big| \\ &= \Big| \sum_{n=N[\frac{x}{N}]+1}^{x} \chi(n) \Big| \leq |x - N[\tfrac{x}{N}]| \leq N = O(1) \end{aligned}$$

wegen Satz 2, §5; deswegen ist nach Satz 2 von §1 die Konvergenzabszisse von $L(s,\chi)$ kleiner oder gleich 0 (offensichtlich sogar gleich 0); insbesondere definiert (1) eine in $\sigma > 0$ holomorphe Funktion. In der Tat läßt sich diese Funktion auf ganz $\mathbb{C}$ holomorph fortsetzen und genügt einer Funktionalgleichung analog zu der von $\zeta(s)$ (s. §7).

Der wichtigste Satz über L-Reihen ist die Tatsache, daß der Wert von $L(1,\chi)$ (der nach dem eben Gesagten definiert ist) stets von Null verschieden ist; hieraus kann man leicht die Existenz unendlich vieler Primzahlen in arithmetischen Folgen schließen. Wir beweisen jetzt diese beiden Ergebnisse.

SATZ: *Sei χ ein von χ_0 verschiedener Dirichletscher Charakter. Dann ist*

$$L(1,\chi) \neq 0 \; . \tag{4}$$

Aufgaben

1. Man beweise elementar die Existenz unendlich vieler Primzahlen der Gestalt $4n - 1$ bzw. $4n + 1$, indem man unter der Annahme, es gäbe nur endlich viele, die Zahlen

$$4 \prod_{p \equiv 3 \,(\mathrm{mod}\, 4)} p - 1 \quad \text{bzw.} \quad 4 \prod_{p \equiv 1 \,(\mathrm{mod}\, 4)} p^2 + 1$$

bildet und einen Widerspruch ableitet. Für welche anderen arithmetischen Folgen gibt es einen analogen Beweis?

2. Man zeige, daß für jeden Dirichletschen Charakter χ

$$\frac{1}{L(s,\chi)} = \sum_{n=1}^{\infty} \frac{\mu(n)\,\chi(n)}{n^s} \qquad (\sigma > 1)$$

ist, wobei $\mu(n)$ die in §2 eingeführte Möbiussche Funktion bezeichnet. Kann man aus dem Satz dieses Paragraphen schließen, daß die Reihe für $s = 1$ konvergiert?

§7 Werte von Dirichletschen Reihen, insbesondere von L-Reihen, an negativen ganzen Stellen

In §4 haben wir gesehen, daß die Riemannsche Zetafunktion $\zeta(s)$ für alle geraden Argumente $s > 1$ und für alle ganzzahligen Argumente $s < 1$ Werte annimmt, die man in geschlossener Gestalt angeben kann; für $s < 1$ sind diese Werte stets rational und in der Hälfte der Fälle gleich Null. Ähnliche Eigenschaften gelten für alle Dirichletschen L-Reihen. Da diese Reihen Funktionalgleichungen erfüllen, braucht man die Werte nur für $s \geq 1$ oder für $s \leq 0$ zu berechnen. Überraschenderweise stellt sich heraus, daß die Werte an den negativen ganzzahligen Stellen trotz der Nichtkonvergenz der Reihen wesentlich einfacher auszurechnen sind als die an positiven ganzzahligen Stellen. Dies liegt an folgendem Satz, welcher es ermöglicht, unter sehr allgemeinen Voraussetzungen Werte von Dirichtletschen Reihen für ganzzahlige negative Argumente zu bestimmen.

SATZ 1: *Sei* $\varphi(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ *eine Dirichletsche Reihe, die für mindestens einen* (komplexen) *Wert von* s *konvergiert, und sei* $f(t) = \sum_{n=1}^{\infty} a_n e^{-nt}$ *die entsprechende Exponentialreihe* (welche für alle $t > 0$ konvergiert). *Hat*

$f(t)$ *für* $t \to 0$ *die asymptotische Entwicklung*

$$(1) \qquad f(t) \sim b_0 + b_1 t + b_2 t^2 + \ldots \qquad (t \to 0) ,$$

so läßt sich $\varphi(s)$ *holomorph in die ganze komplexe Ebene fortsetzen und es gilt*

$$(2) \qquad \varphi(-n) = (-1)^n \, n! \, b_n \qquad (n = 0, 1, 2, \ldots) .$$

Allgemeiner, wenn $f(t)$ *für* $t \to 0$ *die asymptotische Entwicklung*

$$(3) \qquad f(t) \sim \frac{b_{-1}}{t} + b_0 + b_1 t + b_2 t^2 + \ldots$$

besitzt, so hat $\varphi(s)$ *eine meromorphe Fortsetzung, die Funktion* $\varphi(s) - \frac{b_{-1}}{s-1}$ *ist ganz, und die Werte* $\varphi(0)$, $\varphi(-1)$, ... *werden nach wie vor durch die Formel (2) gegeben.*

Bemerkungen: 1. "Asymptotische Entwicklung" bedeutet, daß für jede natürliche Zahl N die Abschätzung

$$(4) \qquad \left| f(t) - \sum_{n<N} b_n t^n \right| \leq C t^N \qquad (0 < t < t_0)$$

gilt (kurz: $f(t) = \sum_{n<N} b_n t^n + O(t^N)$). Insbesondere ist (1) erfüllt, falls $f(t)$ im Punkt $t = 0$ analytisch ist und die Taylor-Entwicklung $\sum_{n=0}^{\infty} b_n t^n$ hat; i.a. wird aber nicht verlangt, daß die Reihe $\sum_{n=0}^{\infty} b_n t^n$ konvergiert, noch, falls sie das tut, daß ihr Wert gleich $f(t)$ ist.

2. Wie aus dem Beweis ersichtlich sein wird, gilt der Satz auch für allgemeine Dirichletsche Reihen $\varphi(s) = \sum_{n=0}^{\infty} \frac{a_n}{\lambda_n^s}$ (falls sie für mindestens ein s absolut konvergieren), wenn man $f(t) = \sum_{n=0}^{\infty} a_n e^{-\lambda_n t}$ setzt.

Beweis des Satzes: Es ist klar, daß die Reihe für $f(t)$ für alle positiven Werte von t absolut konvergiert, da die a_n höchstens polynomial wachsen und die e^{-nt} exponentiell abfallen. Wegen Gleichung (16) von §3 (bzw. Gleichung (18) von §3 im Falle von allgemeinen Dirichletschen Reihen) gilt im Bereich der absoluten Konvergenz die Formel

$$\Gamma(s)\varphi(s) = \int_0^{\infty} f(t) t^{s-1} \, dt .$$

Wir zerlegen das Integral als $I_1(s) + I_2(s)$ mit

$$I_1(s) = \int_0^1 f(t)t^{s-1}\,dt\ ,\quad I_2(s) = \int_1^\infty f(t)t^{s-1}\,dt\ .$$

Da $f(t)$ für $t \to \infty$ exponentiell abfällt (nämlich $f(t) = O(e^{-t})$ bzw. $f(t) = O(e^{-\lambda_0 t})$), konvergiert das zweite Integral für alle s, und zwar absolut und gleichmäßig auf kompakten Mengen, es stellt also eine ganze Funktion von s dar. Weiter gilt

$$\int_0^1 \Big(\sum_{n<N} b_n t^n\Big)\, t^{s-1}\,dt = \sum_{n<N} b_n \frac{t^{n+s}}{n+s}\Big|_0^1 = \sum_{n<N} \frac{b_n}{n+s} \qquad (\sigma > 1)\ ,$$

also

$$I_1(s) = \sum_{n<N} \frac{b_n}{n+s} + \int_0^1 \Big(f(t) - \sum_{n<N} b_n t^n\Big)\, t^{s-1}\,dt \qquad (\sigma > 1)\ ,$$

wobei das Integral wegen (4) für alle s mit $\mathrm{Re}(s) > -N$ absolut und auf kompakten Mengen gleichmäßig konvergiert, also in diesem Gebiet eine holomorphe Funktion darstellt. Die Funktion $\Gamma(s)\varphi(s) - \sum_{n<N} \frac{b_n}{n+s}$ hat also eine holomorphe Fortsetzung in die Halbebene $\mathrm{Re}(s) > -N$. Da N beliebig groß gewählt werden kann, folgt, daß $\Gamma(s)\varphi(s)$ eine meromorphe Fortsetzung auf ganz $\mathbb{C}$ hat, die bis auf (eventuelle) einfache Pole bei $s = -n$ ($n = -1, 0, 1, 2, \ldots$) mit Residuum b_n holomorph ist. Da die Funktion $1/\Gamma(s)$ ganz ist und für $s = 0$, $s = -1$, $s = -2$, ... verschwindet, ist $\varphi(s)$ bis auf einen einfachen Pol bei $s = 1$ mit dem Residuum b_{-1} holomorph. Durch Vergleich der Residuen von $\Gamma(s)\varphi(s)$ und $\Gamma(s)$ (vgl. Aufgabe 3, §3) erhält man die Werte (2).

Als erstes Beispiel nehmen wir $\varphi(s) = \zeta(s)$, die Riemannsche Zetafunktion. Hier ist $a_n = 1$, also

$$f(t) = \sum_{n=1}^\infty e^{-nt} = \frac{1}{e^t - 1}$$

mit der asymptotischen Entwicklung (hier sogar konvergent für $t < 2\pi$)

$$f(t) \sim \frac{1}{t} + \sum_{n=0}^\infty \frac{B_{n+1}}{(n+1)!}\, t^n\ ,$$

und der Satz gibt sofort die holomorphe Fortsetzung von $\zeta(s) - \frac{1}{s-1}$

auf die ganze Ebene sowie die in §4 erhaltenen Werte

$$\zeta(-n) = (-1)^n \frac{B_{n+1}}{n+1} = \begin{cases} -\frac{1}{2} & (n = 0) , \\ -\frac{B_{n+1}}{n+1} & (n \geq 1,\ n \text{ ungerade}) , \\ 0 & (n \geq 2,\ n \text{ gerade}) . \end{cases}$$

Wir betrachten jetzt einen Dirichletschen Charakter $\chi \pmod N$ und setzen $a_n = \chi(n)$, $\varphi(s) = L(s,\chi)$ in Satz 1. Wegen der Periodizität der Koeffizienten gilt dann

$$\begin{aligned} f(t) &= \sum_{n=1}^{\infty} \chi(n)\, e^{-nt} \\ &= \sum_{m=1}^{N} \chi(m) \left(e^{-mt} + e^{-(m+N)t} + e^{-(m+2N)t} + \ldots\right) \\ &= \sum_{m=1}^{N} \chi(m)\, \frac{e^{-mt}}{1-e^{-Nt}} . \end{aligned}$$

Die Funktion e^{-mt} hat für $t \to 0$ die asymptotische Entwicklung $\sum_{k=0}^{\infty} \frac{(-m)^k}{k!} t^k$ und die Funktion $\frac{1}{1-e^{-Nt}}$ hat die Entwicklung $\sum_{r=0}^{\infty} \frac{(-1)^r B_r}{r!} (Nt)^{r-1}$, wobei die B_r Bernoullische Zahlen sind (s. (4.7)). Es gilt also

$$f(t) \sim \sum_{m=1}^{N} \chi(m) \sum_{k=0}^{\infty} \sum_{r=0}^{\infty} \frac{(-1)^{k+r} m^k N^{r-1} B_r}{r!\, k!} t^{r+k-1} ,$$

d.h. eine asymptotische Entwicklung der Gestalt (3) mit

$$b_n = \sum_{m=1}^{N} \chi(m) \sum_{\substack{k,r \geq 0 \\ k+r=n+1}} \frac{(-1)^{k+r} B_r m^k N^{r-1}}{k!\, r!} \qquad (n \geq -1) . \tag{5}$$

Für $n = -1$ reduziert sich diese Summe auf

$$b_{-1} = \frac{1}{N} \sum_{m=1}^{N} \chi(m) ,$$

was für $\chi \neq \chi_0$ verschwindet (§5, Satz 2); nach Satz 1 läßt sich also $L(s,\chi)$ in diesem Fall zu einer für alle s holomorphen Funktion fortsetzen. Für $\chi = \chi_0$ ist

$$b_{-1} = \frac{1}{N} \sum_{\substack{m=1 \\ (m,N)=1}}^{N} 1 = \frac{\phi(N)}{N}$$

und $L(s,\chi)$ hat einen einfachen Pol mit Residuum $\frac{\phi(N)}{N}$ bei $s = 1$, in Übereinstimmung mit (6.3).

Wir können (5) etwas bequemer schreiben, wenn wir die durch

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_{n-k}\, x^k \tag{6}$$

definierten *Bernoullischen Polynome* einführen, also

$$\begin{aligned} B_0(x) &= 1 \ , \\ B_1(x) &= x - \tfrac{1}{2} \ , \\ B_2(x) &= x^2 - x + \tfrac{1}{6} \ , \\ B_3(x) &= x^3 - \tfrac{3}{2} x^2 + \tfrac{1}{6} x \ , \\ &\vdots \end{aligned}$$

Dann ist nämlich

$$b_n = \frac{(-1)^{n+1}}{(n+1)!}\, N^n \sum_{m=1}^{N} \chi(m)\, B_{n+1}\left(\tfrac{m}{N}\right) \ ,$$

und wir erhalten aus Satz 1 den

SATZ 2: *Sei* χ *ein Dirichletscher Charakter modulo* N *und* $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ $(\mathrm{Re}(s) > 1)$ *die entsprechende L-Reihe. Dann läßt sich* $L(s,\chi)$ *meromorph auf die ganze Ebene fortsetzen, und zwar holomorph bis auf einen einfachen Pol mit Residuum* $\frac{\phi(N)}{N}$ *bei* $s = 1$ *für* $\chi = \chi_0$, *und es gilt*

$$L(-n,\chi) = -\frac{N^n}{n+1} \sum_{m=1}^{N} \chi(m)\, B_{n+1}\left(\tfrac{m}{N}\right) \qquad (n = 0, 1, 2, \ldots) \ . \tag{7}$$

Als Beispiel des Satzes haben wir

$$L(0,\chi) = -\frac{1}{N} \sum_{m=1}^{N} \chi(m)\, m \qquad (\chi \neq \chi_0) \ . \tag{8}$$

Die Bernoullischen Polynome, die in der Mathematik in vielen Zusammenhängen vorkommen, haben sehr schöne Eigenschaften. Aus (6) erhält man sofort die Formeln

$$B_n(0) = B_n \ , \tag{9}$$

$$\frac{d}{dx} B_n(x) = n\, B_{n-1}(x) \tag{10}$$