

Analytische Zahlentheorie

Dietrich Burde

Vorlesungsskript 2005

Contents

Einleitung	1
Chapter 1. Elementare Primzahltheorie	5
1.1. Euklid und die Primzahlen	5
1.2. Arithmetische Funktionen	12
1.3. Das Dirichlet-Produkt	18
1.4. Die Eulersche Summationsformel	27
1.5. Ein Taubersatz von Shapiro	32
1.6. Über die Primzahlverteilung	36
Chapter 2. Periodische arithmetische Funktionen und Gauß-Summen	45
2.1. Dirichlet-Charaktere	45
2.2. Endliche Fourier-Reihen	50
2.3. Ramanujan-Summen	52
2.4. Gauß-Summen zu Dirichlet-Charakteren	57
2.5. Pólyas Ungleichung für Dirichlet-Charaktere	62
2.6. Quadratische Gauß-Summen	65
2.7. Kubische Gauß-Summen	71
2.8. Die Kummersche Vermutung	77
2.9. Primzahlen in arithmetischen Progressionen	80
Chapter 3. Dirichlet-Reihen, Riemannsches ζ -Funktion und L -Reihen	93
3.1. Dirichlet-Reihen	93
3.2. Euler-Produkte	97
3.3. Analytische Fortsetzung von $\zeta(s)$	99
3.4. Die Funktionalgleichung für $\zeta(s)$ und $L(s, \chi)$	102
3.5. Die Nullstellen von $\zeta(s)$	105
Bibliography	109

Einleitung

Wie sagte Hardy immer - jeder Dummkopf kann Fragen über Primzahlen stellen, auf die auch der klügste Mensch keine Antwort hat. PAUL ERDÖS.

Dieses Skript ist entstanden für eine einführende Vorlesung über analytische Zahlentheorie an der Universität Wien.

In der Zahlentheorie beschäftigt man sich mit den Eigenschaften der ganzen Zahlen. Historisch gesehen ist das wahrscheinlich die erste mathematische Disziplin. Schon die Sumerer (2500 v.Chr.) und die Babylonier (2000 v.Chr.) haben die natürlichen Zahlen untersucht und einen Kalender entworfen. Der erste wissenschaftliche Ansatz wird den alten Griechen zugesprochen. Pythagoras und seine Schule (600 v.Chr.) hatten bereits beachtliche Überlegungen angestellt. EUKLID war einer der ersten Wissenschaftler, die mathematische Tatsachen auch mit einem rigorosen Beweis präsentierten. Seine Bücher, zusammengefaßt als *die Elemente* stellen ein wichtiges Werk dar. Dort wird unter anderem auch auf die Grundbausteine (die Atome sozusagen) der ganzen Zahlen eingegangen, den *Primzahlen*. Euklid beweist dort, daß es unendlich viele Primzahlen gibt. Das war der Anfang einer langen Entdeckungsreise durch das Reich der Primzahlen. Heute ist die Zahlentheorie eine der hochentwickeltsten Disziplinen. Großartige Entdeckungen in der Primzahltheorie sind gemacht worden, wie etwa der Primzahlsatz. Dennoch sind immer noch viele bekannte Vermutungen offen, die wichtigste davon wahrscheinlich die Riemannsche Vermutung.

Hier ist der Versuch einer Liste derjenigen Mathematiker, deren Name im Zusammenhang mit analytischer Zahlentheorie nicht fehlen sollte:

Viggo Brun (1885-1978),
Pafnuty Lvovich Chebyshev (1821-1894),
Johann Peter Gustav Lejeune Dirichlet (1805-1859),
Paul Erds (1913-1996),
Leonhard Euler (1707-1783),
Pierre de Fermat (1601-1665),
Carl Friedrich Gau (1777-1855),
Jacques Salomon Hadamard (1865-1963),
Godfrey Harold Hardy (1877-1947),
Carl Gustav Jacob Jacobi (1804-1851),
Edmund Georg Hermann Landau (1877-1938),
Charles Jean Gustave Nicolas Baron de la Valle Poussin
(1866-1962),
Adrien-Marie Legendre (1752-1833),
Hans von Mangoldt (1854-1925),
Franz Mertens (1840-1927),

Srinivasa Aiyangar Ramanujan (1887–1920)
 Georg Friedrich Bernhard Riemann (1826–1866),
 Atle Selberg (1917–),
 Carl Ludwig Siegel (1896–1981)
 Ivan Matveevich Vinogradov (1891–1983).

In Bezug auf obigen Ausspruch von Erdős haben wir einige Beispiele von Fragen über Primzahlen zusammengetragen, die man leicht stellen, aber nur schwer beantworten kann:

- Wieviele Primzahlen gibt es und wie sind sie verteilt ?
- Ist jede gerade Zahl $n \geq 4$ die Summe zweier Primzahlen ?
- Wieviele Primzahlzwillinge gibt es ?
- Liegt zwischen zwei Quadratzahlen mindestens eine Primzahl ?
- Wieviele Primzahlen gibt es in arithmetischen Folgen $a_n = kn + h$ mit $(h, k) = 1$?
- Wieviele Mersenne-Primzahlen der Form $2^n - 1$ gibt es ? Wieviele Fermat-Primzahlen der Form $2^{2^n} + 1$ gibt es ?
- Wieviele Primzahlen der Form $n^2 + 1$, $n! - 1$ oder $n! + 1$ gibt es ?

Einige dieser Fragen sind berühmte Vermutungen. Wir diskutieren hier insbesondere die Fragen zur Primzahlverteilung, und zwar hauptsächlich mit analytischen Methoden.

Es gibt natürlich noch viel mehr Fragen über Primzahlen, aber nicht alle sind wirklich interessant (sondern vielleicht eher kurios). Eine davon ist die Frage nach Primzahlen, deren Ziffern sämtlich ebenfalls Primzahlen sind. Die ersten solchen Primzahlen sind

2, 3, 5, 7, 23, 37, 53, 73, 223, 227, 233, 257, 277, 337, 353, 373, 523, 557, ...

Die Folge dieser Zahlen hat den Namen A019546 in Sloane's Katalog. Die Liste der palindromischen Primzahlen (Sloane's A002385) beginnt mit

2, 3, 5, 7, 11, 101, 131, 151, 181, 191, 313, 353, 373, 383, 727, 757, 787, 797,
 919, 929, 10301, 10501, 10601, 11311, 11411, ...

Die Summe $\sum_p \frac{1}{p}$ über alle palindromischen Primzahlen konvergiert, und zwar ungefähr gegen 1.32398. Die ersten palindromischen Primzahlen, die in der Dezimalentwicklung von π auftauchen, sind 3, 313 und

31415926535897932384626433833462648323979853562951413.

Beeindruckend sind auch folgende Pyramiden palindromischer Primzahlen (G. L. Honaker und M. Kenn):

2

30203

133020331

1713302033171

12171330203317121

151217133020331712151

1815121713302033171215181

16181512171330203317121518161

331618151217133020331712151816133

9333161815121713302033171215181613339

11933316181512171330203317121518161333911

5

97579

389757983

3138975798313

15313897579831351

741531389757983135147

9074153138975798313514709

73907415313897579831351470937

907390741531389757983135147093709

3690739074153138975798313514709370963

38369073907415313897579831351470937096383

393836907390741531389757983135147093709638393

7039383690739074153138975798313514709370963839307

71703938369073907415313897579831351470937096383930717

347170393836907390741531389757983135147093709638393071743

9534717039383690739074153138975798313514709370963839307174359

93953471703938369073907415313897579831351470937096383930717435939

799395347170393836907390741531389757983135147093709638393071743593997

3679939534717039383690739074153138975798313514709370963839307174359399763

14367993953471703938369073907415313897579831351470937096383930717435939976341

761436799395347170393836907390741531389757983135147093709638393071743593997634167

177614367993953471703938369073907415313897579831351470937096383930717435939976341677

70177614367993953471703938369073907415313897579831351470937096383930717435939976341677

Zum Schluß möchte ich noch allen danken, die mich auf Tippfehler und Irrtümer aufmerksam gemacht haben.

CHAPTER 1

Elementare Primzahltheorie

In diesem einführenden Kapitel geht es um Resultate über Primzahlen und ihre Verteilung, die mit elementaren Methoden (also ohne komplexe Analysis) und ohne großen Aufwand bewiesen werden können.

1.1. Euklid und die Primzahlen

Wir beginnen mit einigen Definitionen und Standardnotationen.

DEFINITION 1.1.1. Sei R ein kommutativer Ring mit 1. Ein Element $p \in R$ heißt *prim*, falls es keine Einheit ist und aus $p \mid ab$ folgt $p \mid a$ oder $p \mid b$. Es heißt *irreduzibel*, falls es keine Einheit ist und keine Zerlegung $p = ab$ in echte Faktoren $a, b \in R$ hat.

Da $R = \mathbb{Z}$ ein Hauptidealring ist, bedeutet die Primalität von p in \mathbb{Z} genau die Irreduzibilität von p in \mathbb{Z} . Mit anderen Worten, eine natürliche Zahl p ist genau dann prim, wenn sie nur durch ± 1 oder $\pm p$ teilbar ist. Es ist natürlich, sich auf die positiven Teiler zu beschränken. Damit erhält man die übliche Definition einer Primzahl. Die Menge der Primzahlen in \mathbb{N} wird mit \mathbb{P} bezeichnet. Ganze Zahlen, die nicht prim sind, heißen *zusammengesetzt*. Es gilt der folgende wichtige Fundamentalsatz der Arithmetik (FDA):

THEOREM 1.1.2 (FDA). *Zu jeder natürlichen Zahl n existieren eindeutig bestimmte Zahlen $e(p) \in \mathbb{N}_0$, so daß gilt*

$$n = \prod_{p \in \mathbb{P}} p^{e(p)}$$

Insbesondere sind nur endlich viele der Zahlen $e(p)$ von Null verschieden.

Hierbei interpretieren wir $n = 1$ als das leere Produkt. Die Existenz einer solchen Darstellung ergibt sich durch Induktion über n ; die Eindeutigkeit folgt mehr oder weniger aus der Eigenschaft $p \mid ab \Rightarrow p \mid a \vee p \mid b$ für Primzahlen $p \in \mathbb{N}$.

BEMERKUNG 1.1.3. Der erste rigorose Beweis des FDA wurde erst 1801 von Gauß gegeben, in seinen *Disquisitiones arithmeticae*. Ringtheoretisch besagt der Satz, daß \mathbb{Z} ein faktorieller Ring ist. Es ist wohlbekannt, daß viele andere Ringe in der Zahlentheorie nicht faktoriell sind. Dazu betrachtet man zum Beispiel die Ringe \mathcal{O}_d der ganzen Zahlen eines quadratischen Zahlkörpers $\mathbb{Q}[\sqrt{d}]$ für quadratfreie $d \in \mathbb{Z}$. Es gilt $\mathcal{O}_d = \mathbb{Z}[\alpha]$, mit $\alpha = \sqrt{d}$ für $d \equiv 2, 3 \pmod{4}$ und $\alpha = \frac{1+\sqrt{d}}{2}$ für $d \equiv 1 \pmod{4}$. Diese Ringe sind genau dann faktoriell wenn sie Hauptidealringe sind, also Klassenzahl 1 haben. Als Beispiel eines solchen Ringes ohne eindeutige Primfaktorzerlegung betrachte man $R = \mathbb{Z}[\sqrt{-5}]$. Dann sind etwa die Elemente $2, 3, 1 \pm \sqrt{-5}$ alle prim, aber

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$$

stellt zwei wesentlich verschiedene Primfaktorzerlegungen von $n = 6$ in R dar. Und in der Tat, dieser Ring hat Klassenzahl 2, also verschieden von 1. Für imaginär-quadratische Zahlkörper

ist genau bekannt, für welche (quadratfreien) $d < 0$ die Ringe \mathcal{O}_d faktoriell sind; nämlich genau für

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Im Umkehrschluß folgt dann, daß zum Beispiel die Ringe \mathcal{O}_d für

$$d = -5, -6, -10, -13, -14, -15, -17, -21, -22, -23, -26, -29, -30, \dots$$

nicht faktoriell sind. Man versuche einmal, dafür konkrete Beispiele zu finden, die die Faktorialität widerlegen, so wie im Fall $d = -5$ oben. Hier ist noch ein Beispiel: in $R = \mathbb{Z}[\sqrt{-26}]$ sind die Elemente $3, 1 \pm \sqrt{-26}$ alle prim und

$$27 = 3 \cdot 3 \cdot 3 = (1 - \sqrt{-26}) \cdot (1 + \sqrt{-26})$$

stellt zwei wesentlich verschiedene Primfaktorzerlegungen von $n = 27$ dar.

Für reell-quadratische Zahlkörper, also für $d > 0$, ist nicht genau bekannt, welche Ringe \mathcal{O}_d faktoriell sind. Es sind aber viel mehr als im Fall $d < 0$. Die Vermutung von Gauß besagt, daß es unendlich viele sind. Hier ist die Liste der $1 \leq d \leq 70$ für die die Ringe \mathcal{O}_d nicht faktoriell sind (die Klassenzahl ist jedesmal gleich zwei):

$$d = 10, 15, 26, 30, 34, 35, 39, 42, 51, 55, 58, 65, 66, 70.$$

Zurück zu der Frage, wieviele Primzahlen es in \mathbb{N} gibt. Dazu führt man eine Zählfunktion ein.

DEFINITION 1.1.4. Sei x eine reelle Zahl. Es bezeichne $\pi(x)$ die Anzahl der Primzahlen p mit $p \leq x$, d.h.,

$$\pi(x) = \sum_{p \leq x} 1.$$

SATZ 1.1.5 (Euklid). *Es gibt unendlich viele Primzahlen, d.h., $\pi(x) \rightarrow \infty$ für $x \rightarrow \infty$.*

BEWEIS. Gäbe es nur endlich viele Primzahlen, so könnten wir sie auflisten: p_1, p_2, \dots, p_r . Dann definiere man

$$N := \prod_{i=1}^r p_i + 1.$$

Wegen Satz 1.1.2 kann N faktorisiert werden, also muß N durch eine der Primzahlen p_k aus unserer Liste teilbar sein. Da p_k aber auch das Produkt $p_1 \cdots p_r$ teilt, muß p_k auch die Differenz teilen, also $p_k \mid 1$. Das ist absurd. \square

BEMERKUNG 1.1.6. Man kann diesen wunderbaren, einfachen Beweis noch verkürzen. Die folgende Variante benutzt nur vier Symbole:

$$N = n! + 1$$

In der Tat, diese Zahl ist durch kein d mit $2 \leq d \leq n$ teilbar. Also hat sie nur Primfaktoren $p > n$. Somit findet man immer eine Primzahl, die größer ist als alle einer vorher festgelegten endlichen Menge von Primzahlen.

Wir werden im folgenden noch viele andere Beweise für diesen Satz kennenlernen. Einige davon zeigen dann auch noch erheblich mehr (etwa daß die Summe

$$\sum_{p \in \mathbb{P}} \frac{1}{p}$$

divergent ist).

Beweis von Goldbach, 1730: es bezeichne $F_n = 2^{2^n} + 1$ die n -te Fermatzahl. Je zwei verschiedene Fermatzahlen sind prim zueinander: $(F_m, F_n) = 1$ für alle $n \neq m$. Das folgt aus der Rekursionsformel

$$F_0 F_1 \cdots F_{n-1} = F_n - 2,$$

die man leicht mit Induktion beweisen kann. Denn es sei $k \in \mathbb{N}$ mit $k \mid F_n$ und $k \mid F_m$. Dann folgt aus der Formel $k \mid 2$, also $k = 1$ oder $k = 2$. Da aber alle F_n ungerade sind, muß $k = 1$ folgen. Damit sind die Primteiler der Fermatzahlen paarweise verschieden. So erhält man immer neue Primzahlen aus der Folge der F_n .

Dieser Beweis zeigt auch $p_n \leq 2^{2^{n-1}}$ für die n -te Primzahl. Die Beweisidee kann variiert werden. Es genügt, irgendeine Folge (n_i) von paarweise teilerfremden Zahlen zu finden mit $2 \leq n_1 < n_2 < \dots$

Ein weiterer Beweis basiert auf dem folgenden Lemma:

LEMMA 1.1.7. *Sind p_1, p_2, \dots, p_r verschiedene Primzahlen, so gilt*

$$(1.1) \quad \prod_{k=1}^r \left(1 - \frac{1}{p_k}\right)^{-1} = \sum_{n \in \mathcal{N}(p_1, \dots, p_r)} \frac{1}{n}$$

wobei $\mathcal{N}(p_1, \dots, p_r)$ die Menge der $n \in \mathbb{N}$ ist, für die gilt:

$$p \mid n \Rightarrow p = p_i \text{ für ein } i \leq r.$$

BEWEIS. Man entwickle jeden Faktor des Produkts in eine geometrische Reihe:

$$\frac{1}{1 - \frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \dots$$

Damit folgt dann

$$\begin{aligned} \prod_{k=1}^r \left(1 - \frac{1}{p_k}\right)^{-1} &= \prod_{k=1}^r \left(\sum_{\ell=0}^{\infty} \frac{1}{p_k^\ell}\right) \\ &= \sum_{\ell_1=0}^{\infty} \sum_{\ell_2=0}^{\infty} \cdots \sum_{\ell_r=0}^{\infty} \frac{1}{p_1^{\ell_1} \cdots p_r^{\ell_r}} \\ &= \sum_{n \in \mathcal{N}(p_1, \dots, p_r)} \frac{1}{n} \end{aligned}$$

□

Damit erhält man Satz 1.1.5 wie folgt: nach Annahme gibt es nur endlich viele Primzahlen p_1, \dots, p_r . Dann ist wegen des FDA $\mathcal{N}(p_1, \dots, p_r) = \mathbb{N}$. Nach (1.1) gilt also

$$\prod_{k=1}^r \left(1 - \frac{1}{p_k}\right)^{-1} = \sum_{n \in \mathbb{N}} \frac{1}{n}$$

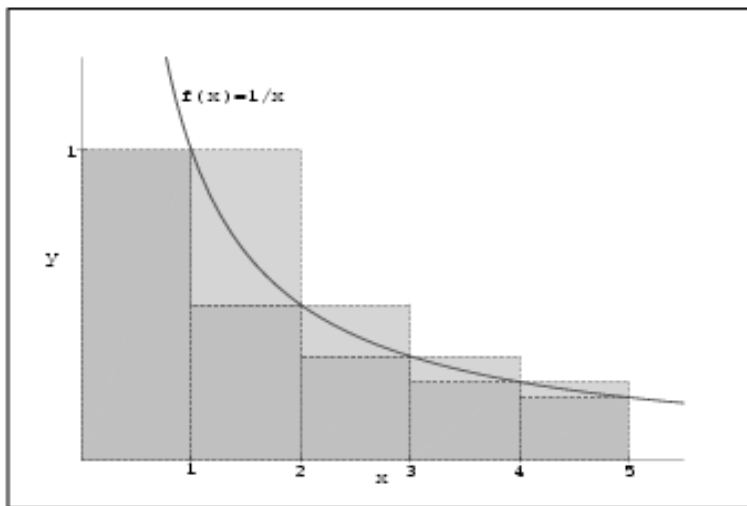
Die linke Seite hiervon ist aber endlich, so daß die harmonische Reihe konvergiert. Das ist ein Widerspruch.

Wir wollen noch einen Beweis präsentieren. Dazu benötigen wir

LEMMA 1.1.8. Für $N \geq 1$ gilt

$$\log(N) < \sum_{n=1}^N \frac{1}{n} \leq \log(N) + 1.$$

BEWEIS. Man betrachte das Integral $\int_1^N \frac{1}{x} dx = \log(N)$ und vergleiche es mit der Unter- und Obersumme.



□

BEMERKUNG 1.1.9. Die Eulersche Konstante ist definiert als

$$\gamma = \lim_{N \rightarrow \infty} \left(\sum_{n \leq N} \frac{1}{n} - \log(N) \right).$$

Sie hat ungefähr den Wert $\gamma \approx 0.577215664$. Die Tatsache, daß die Differenz für jedes N beschränkt bleibt, schreibt man auch gerne wie folgt:

$$\sum_{n \leq x} \frac{1}{n} = \log(x) + O(1)$$

Dabei verwendet man die O -Notation von Landau:

DEFINITION 1.1.10. Es sei $A \subseteq \mathbb{R}$ und $f: A \rightarrow \mathbb{R}$, $g: A \rightarrow \mathbb{R}_+$ zwei Funktionen. Dann schreiben wir

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

falls es eine Konstante $c > 0$ gibt mit $|f(x)| \leq c \cdot g(x)$ für alle $x \in A$.

Eine andere Bezeichnung dafür stammt von Vinogradov: $f(x) \ll g(x)$. Man kann die Definition auch auf komplexe Funktionen ausdehnen, solange das Bild von g in \mathbb{R}_+ liegt.

BEISPIEL 1.1.11. $f(x) = O(1)$ bedeutet, daß f beschränkt ist.

So ist z.B. $\sin(x) = O(1)$. Ein anderes Beispiel ist $e^{-x} = O(x^{-n})$ für jedes $n \in \mathbb{N}$.

Beweis von Satz 1.1.5: Sei $x \geq 2$ beliebig, und seien p_1, \dots, p_r die Primzahlen p mit $p \leq x$. Nach dem FDA umfaßt $\mathcal{N}(p_1, \dots, p_r)$ dann zumindest die Menge $\{1, 2, \dots, [x]\}$. Dann folgt mit Lemma 1.1.8 und analog zu (1.1)

$$(1.2) \quad \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} \geq \sum_{n \leq x} \frac{1}{n} > \log(x).$$

Hierbei hat man $\log(x) \rightarrow \infty$ für $x \rightarrow \infty$. Damit kann das Produkt nicht endlich bleiben für $x \rightarrow \infty$.

Dieser Beweis liefert sogar noch mehr:

SATZ 1.1.12. Für $x \geq 2$ gilt

$$\sum_{p \leq x} \frac{1}{p} > \log(\log(x)) - 1.$$

Insbesondere ist die Reihe $\sum_p \frac{1}{p}$ divergent.

Zum Beweis wird folgendes Lemma benötigt.

LEMMA 1.1.13. Für alle $t \in [0, \frac{1}{2}]$ gilt $\frac{1}{1-t} \leq e^{t+t^2}$.

BEWEIS. Man setze $f(t) = (1-t) \exp(t+t^2)$. Die Behauptung ist nun, daß $f(t) \geq 1$ ist für alle $t \in [0, \frac{1}{2}]$. Nun ist $f(0) = 1$, und die Funktion aber monoton steigend auf dem Intervall, wegen $f'(t) = t(1-2t) \exp(t+t^2) \geq 0$ für alle $t \in [0, \frac{1}{2}]$. Daraus folgt die Behauptung. \square

Beweis von Satz 1.1.12: Man verwende (1.2) und wende das Lemma für $t = \frac{1}{p} \in (0, \frac{1}{2}]$ an. Dann erhält man

$$\log(x) < \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} < \prod_{p \leq x} \exp\left(\frac{1}{p} + \frac{1}{p^2}\right).$$

Wegen der Monotonie des Logarithmus folgt daraus

$$\log(\log(x)) < \sum_{p \leq x} \left(\frac{1}{p} + \frac{1}{p^2}\right) < \sum_{p \leq x} \frac{1}{p} + \sum_{p \in \mathbb{P}} \frac{1}{p^2}.$$

Die zweite Reihe bleibt aber kleiner als eins wegen

$$\sum_{p \in \mathbb{P}} \frac{1}{p^2} < \sum_{n=2}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} - 1 < 1.$$

Der Wert der Reihe ist übrigens ungefähr 0.45224742. \square

BEMERKUNG 1.1.14. Man kann zeigen, daß für $x \geq 2$ auch folgendes gilt [16]:

$$\sum_{p \leq x} \frac{1}{p} = \log(\log(x)) + c + O\left(\frac{1}{\log x}\right)$$

Dabei ist die Konstante c gegeben durch

$$c = \gamma - \sum_{p \in \mathbb{P}} \left(\log\left(\frac{1}{1 - \frac{1}{p}}\right) - \frac{1}{p} \right) \approx 0.2614972128.$$

Das folgende Resultat von Euler kann vielleicht als die Geburtsstunde der analytischen Zahlentheorie angesehen werden. Es verallgemeinert den FDA:

SATZ 1.1.15 (Euler). Für $\sigma > 1$ gilt

$$\sum_{n=1}^{\infty} \frac{1}{n^{\sigma}} = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^{\sigma}}\right)^{-1}.$$

BEWEIS. Es sei $\sigma > 0$. Dann folgt völlig analog zu (1.1)

$$\prod_{p \leq x} \left(1 - \frac{1}{p^{\sigma}}\right)^{-1} = \sum_{\substack{n \in \mathbb{N} \\ p|n \Rightarrow p \leq x}} \frac{1}{n^{\sigma}}$$

Für $\sigma > 1$ folgt mit $x \rightarrow \infty$ die Behauptung. □

Natürlich folgt hieraus erneut, daß es unendlich viele Primzahlen gibt, indem man $\sigma \rightarrow 1$ gehen läßt. Die Reihe in Eulers Satz ist von großer Bedeutung. Es war Riemann, der den Einfall hatte, diese Reihe auch für komplexe Variablen zu betrachten:

DEFINITION 1.1.16. Für $s = \sigma + it$, $\sigma > 1$ ist die *Riemannsche Zetafunktion* definiert durch

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

SATZ 1.1.17. Die Reihe ist für alle $s = \sigma + it$ mit $\sigma > 1$ absolut konvergent, und in jeder Halbebene $\sigma \geq \sigma_0 > 1$ gleichmäßig konvergent. Damit ist $\zeta(s)$ für $\operatorname{Re}(s) > 1$ eine holomorphe Funktion.

BEWEIS. Wegen $|n^s| = n^{\sigma}$ gilt

$$\left| \sum_{n=1}^{\infty} \frac{1}{n^s} \right| \leq \sum_{n=1}^{\infty} \frac{1}{n^{\sigma}} \leq \sum_{n=1}^{\infty} \frac{1}{n^{\sigma_0}} < 1 + \int_1^{\infty} \frac{dt}{t^{\sigma_0}} = 1 + \frac{1}{\sigma_0 - 1}$$

Damit folgt die behauptete Konvergenz. Also ist $\zeta(s)$ als Grenzfunktion einer gleichmäßig konvergenten Folge holomorpher Funktionen selbst holomorph. Das besagt der Satz von Weierstrass. □

Die Zetafunktion spielt eine zentrale Rolle in der Zahlentheorie. Wir werden sie später noch genauer studieren. Die Identität von Euler gilt auch für komplexe s mit $\operatorname{Re}(s) > 1$, wie wir noch sehen werden.

SATZ 1.1.18. Für $s \in \mathbb{C}$ mit $\operatorname{Re}(s) > 1$ gilt

$$\zeta(s) = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Wir wollen noch einen weiteren Beweis dafür geben, daß die Reihe der reziproken Primzahlen divergiert. Er verwendet die Identität von Euler.

Beweis von Satz 1.1.12: Für $\sigma > 1$ gilt

$$\begin{aligned}\log(\zeta(\sigma)) &= -\sum_p \log\left(1 - \frac{1}{p^\sigma}\right) = -\sum_p \sum_{m=1}^{\infty} -\frac{1}{mp^{m\sigma}} \\ &= \sum_p \frac{1}{p^\sigma} + \sum_p \sum_{m=2}^{\infty} \frac{1}{mp^{m\sigma}}.\end{aligned}$$

Wir sind fertig, wenn wir zeigen, daß die Doppelsumme beschränkt ist. Denn dann haben wir

$$\log(\zeta(\sigma)) = \sum_p \frac{1}{p^\sigma} + O(1),$$

wobei die linke Seite für $\sigma \rightarrow 1$ divergiert. Also folgt $\sum_p \frac{1}{p} = \infty$. Nun ist aber, wegen $1 - \frac{1}{p^{2\sigma}} \geq \frac{1}{2}$ und $\sigma > 1$:

$$\sum_p \sum_{m=2}^{\infty} \frac{1}{mp^{m\sigma}} < \sum_p \sum_{m=2}^{\infty} \frac{1}{p^{m\sigma}} = \sum_p \frac{1}{p^{2\sigma}} \cdot \frac{1}{1 - \frac{1}{p^{2\sigma}}} < 2 \sum_p \frac{1}{p^{2\sigma}} \leq 2 \sum_p \frac{1}{p^2}.$$

□

1.2. Arithmetische Funktionen

Arithmetische, oder zahlentheoretische Funktionen treten in der Primzahltheorie in natürlicher Weise auf. Man betrachte zum Beispiel die Funktion ω , definiert durch

$$\omega(n) = \sum_{p|n} 1.$$

Sie zählt offensichtlich die positiven Primteiler von n . So ist etwa $\omega(p) = 1$ für alle Primzahlen p .

DEFINITION 1.2.1. Eine *arithmetische Funktion* ist eine Funktion $f: \mathbb{N} \rightarrow \mathbb{C}$. Sie heißt *multiplikativ*, falls $f(1) = 1$, und für alle $n, m \in \mathbb{N}$ mit $(n, m) = 1$ gilt

$$f(mn) = f(m)f(n).$$

Die Funktion heißt *streng multiplikativ*, falls obige Gleichung für alle $n, m \in \mathbb{N}$ gilt.

Die Bedingung $f(1) = 1$ ist dabei nur eine Konvention, die die Nullfunktion ausschließen soll. Ist f streng (oder vollständig) multiplikativ, so gilt $f(p^\alpha) = f(p)^\alpha$.

BEISPIEL 1.2.2. Die Funktion ω ist nicht multiplikativ. Die Funktion

$$\tau(n) = \sum_{d|n} 1$$

ist multiplikativ, aber nicht streng multiplikativ. Die Funktionen $f_s(n) = n^s$, für $s \in \mathbb{C}$, sind streng multiplikativ.

Wäre ω multiplikativ, so hätte man für zwei verschiedene Primzahlen p und q nämlich $1 = \omega(p)\omega(q) = \omega(pq) = 2$. Die Funktion τ zählt die positiven Teiler von n . Wir werden gleich sehen, daß für alle $n \geq 1$ gilt:

$$\tau(n) = \prod_{p^\alpha || n} (\alpha + 1).$$

Hierbei bedeutet $p^\alpha || n$, daß $p^\alpha | n$, aber $p^{\alpha+1} \nmid n$. Das bedeutet, daß τ multiplikativ ist.

DEFINITION 1.2.3. Die Teileranzahlfunktionen σ_k sind definiert durch

$$\sigma_k(n) = \sum_{d|n} d^k.$$

Die Möbiussche μ -Funktion ist definiert durch

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & \text{falls } n \text{ quadratfrei ist,} \\ 0 & \text{sonst.} \end{cases}$$

Die Eulersche φ -Funktion ist definiert durch

$$\varphi(n) = \sum_{\substack{1 \leq k \leq n \\ (k, n) = 1}} 1.$$

Die von Mangoldtische Λ -Funktion ist definiert durch

$$\Lambda(n) = \begin{cases} \log(p) & \text{falls } n = p^m \text{ für ein } m \geq 1 \text{ ist,} \\ 0 & \text{sonst.} \end{cases}$$

Die Funktion $\sigma_1(n) = \sum_{d|n} d$ wird auch mit $\sigma(n)$ bezeichnet.

SATZ 1.2.4. *Die Funktionen τ und σ sind multiplikativ, aber nicht streng multiplikativ. Es gilt nämlich, für $n = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$,*

$$\tau(n) = \prod_{i=1}^{\ell} (\alpha_i + 1),$$

$$\sigma(n) = \prod_{i=1}^{\ell} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

BEWEIS. Es gilt $d \mid n$ genau dann, wenn $d = p_1^{\beta_1} \cdots p_\ell^{\beta_\ell}$ gilt mit $0 \leq \beta_i \leq \alpha_i$ für alle $1 \leq i \leq \ell$. Die positiven Teiler d stehen also in bijektiver Korrespondenz zu den n -Tupeln $(\beta_1, \dots, \beta_\ell)$ mit $0 \leq \beta_i \leq \alpha_i$. Da es für die β_i genau $\alpha_i + 1$ Wahlmöglichkeiten gibt, hat man genau $(\alpha_1 + 1) \cdots (\alpha_\ell + 1)$ solche Tupel.

Um die zweite Formel einzusehen, schreibe man

$$\sigma(n) = \sum_{d|n} d = \sum_{(\beta_1, \dots, \beta_\ell)} p_1^{\beta_1} \cdots p_\ell^{\beta_\ell},$$

wobei über alle Tupel $(\beta_1, \dots, \beta_\ell)$ mit $0 \leq \beta_i \leq \alpha_i$ summiert wird. Diese Summe ist gleich

$$\left(\sum_{\beta_1=0}^{\alpha_1} p_1^{\beta_1} \right) \left(\sum_{\beta_2=0}^{\alpha_2} p_2^{\beta_2} \right) \cdots \left(\sum_{\beta_\ell=0}^{\alpha_\ell} p_\ell^{\beta_\ell} \right) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_\ell^{\alpha_\ell+1} - 1}{p_\ell - 1}.$$

□

BEMERKUNG 1.2.5. Die Formel für $\sigma(n)$ verallgemeinert sich für alle $\sigma_k(n)$, nämlich

$$\sigma_k(n) = \prod_{i=1}^{\ell} \frac{p_i^{k(\alpha_i+1)} - 1}{p_i^k - 1}.$$

Damit sind auch alle Funktionen $\sigma_k(n)$ multiplikativ.

SATZ 1.2.6. *Die Funktion $\mu(n)$ ist multiplikativ, und es gilt*

$$\sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1 & \text{falls } n = 1, \\ 0 & \text{sonst.} \end{cases}$$

BEWEIS. Es gilt $\mu(1) = 1$, $\mu(p_1 \cdots p_\ell) = (-1)^\ell$ für verschiedene Primzahlen p_1, \dots, p_ℓ und $\mu(p^\alpha) = 0$ für $\alpha \geq 2$. Es seien n, m mit $(n, m) = 1$ gegeben. Hat entweder n oder m einen Faktor p^2 , so auch nm und es gilt $\mu(mn) = \mu(m)\mu(n) = 0$. Andernfalls ist wegen $(n, m) = 1$

$$\mu(mn) = (-1)^{\omega(m)+\omega(n)} = (-1)^{\omega(m)}(-1)^{\omega(n)} = \mu(m)\mu(n).$$

Was die Formel betrifft, dürfen wir $n \geq 2$ annehmen. Sei $n = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$ die Primfaktorzerlegung von n . Dann kommen die einzigen von Null verschiedenen Terme in der Summe $\sum_{d|n} \mu(d)$ von

$d = 1$ oder von Produkten von r verschiedenen Primzahlen aus der Menge $\{p_1, \dots, p_\ell\}$. Davon gibt es $\binom{\ell}{r}$ viele:

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + (\mu(p_1) + \dots + \mu(p_\ell)) \\ &\quad + \mu(p_1 p_2) + \mu(p_1 p_3) + \dots + \mu(p_{\ell-1} p_\ell) + \dots + \mu(p_1 p_2 \dots p_\ell) \\ &= 1 + \binom{\ell}{1} (-1)^1 + \binom{\ell}{2} (-1)^2 + \dots + \binom{\ell}{\ell} (-1)^\ell \\ &= (1 - 1)^\ell = 0. \end{aligned}$$

□

KOROLLAR 1.2.7. *Es gilt*

$$\sum_{d|n} \mu^2(d) = 2^{\omega(n)}.$$

BEWEIS. Ersetzt man im obigen Beweis $\mu(d)$ durch $\mu^2(d) = |\mu(d)|$, so erhält man

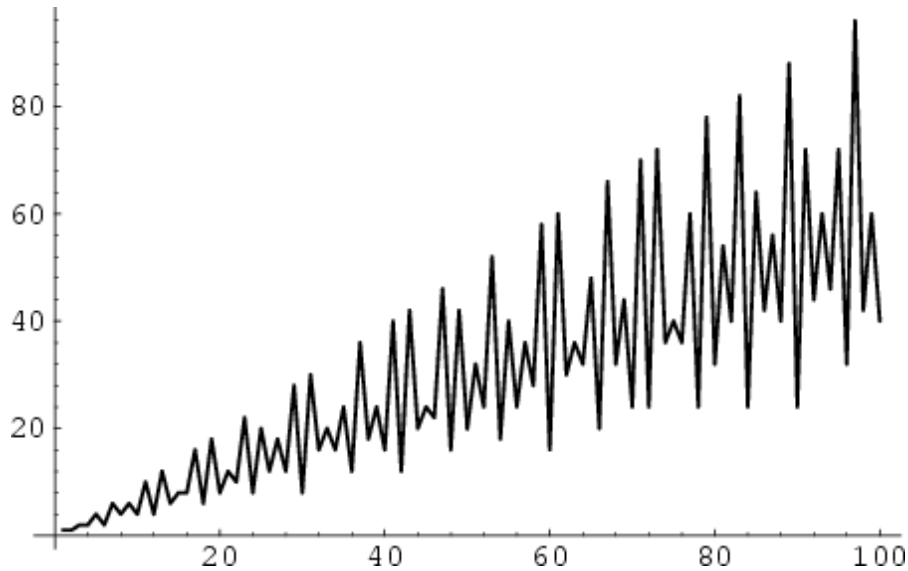
$$\sum_{d|n} \mu^2(d) = \sum_{\ell=0}^{\omega(n)} \binom{\omega(n)}{\ell} = (1 + 1)^{\omega(n)} = 2^{\omega(n)}.$$

□

Kommen wir nun zur Eulerschen φ -Funktion. Da $\varphi(n)$ die Ordnung der Einheitengruppe $E(\mathbb{Z}/n\mathbb{Z})$ ist und bekanntlich für $(m, n) = 1$ gilt

$$E(\mathbb{Z}/n\mathbb{Z}) \times E(\mathbb{Z}/m\mathbb{Z}) \cong E(\mathbb{Z}/nm\mathbb{Z}),$$

so folgt $\varphi(mn) = \varphi(n)\varphi(m)$. Also ist φ multiplikativ. Das folgt allerdings auch direkt aus der Produktformel für $\varphi(n)$, die wir noch herleiten werden. Um sich ein Bild von der φ -Funktion zu machen, betrachte man den Graphen im Bereich von $[1, 100]$:



SATZ 1.2.8. Die Funktion $\varphi(n)$ ist multiplikativ und es gilt

$$\sum_{d|n} \varphi(d) = n.$$

BEWEIS. Sei $S = \{1, 2, \dots, n\}$. Wir verteilen die Zahlen aus S in disjunkte Mengen wie folgt. Für $d | n$ sei

$$A(d) = \{k \in \mathbb{N} \mid 1 \leq k \leq n, (k, n) = d\}.$$

Diese Menge beinhaltet diejenigen Elemente von S , deren ggT mit n gleich d ist. Wir setzen $f(d) = |A(d)|$. Dann gilt

$$\bigcup_{d|n} A(d) = S, \text{ also } \sum_{d|n} f(d) = n.$$

Es ist $(k, n) = d$ gleichwertig mit $(\frac{k}{d}, \frac{n}{d}) = 1$, wobei $0 < k \leq n$ genau dann gilt, wenn $0 < \frac{k}{d} \leq \frac{n}{d}$. Mit $q = \frac{k}{d}$ hat man also eine bijektive Korrespondenz zwischen den Elementen in $A(d)$ und den Elementen in $\{q \in \mathbb{N} \mid 0 < q \leq \frac{n}{d}, (q, \frac{n}{d}) = 1\}$. Die Anzahl solcher q 's ist aber gerade $\varphi(\frac{n}{d})$. Also gilt $f(d) = \varphi(\frac{n}{d})$ und somit

$$\sum_{d|n} \varphi\left(\frac{n}{d}\right) = n.$$

Das ist aber äquivalent zu der Behauptung des Satzes, weil mit d auch $\frac{n}{d}$ alle Teiler von n durchläuft. \square

Die Funktionen $\varphi(n)$ und $\mu(n)$ hängen wie folgt zusammen:

SATZ 1.2.9. Für $n \geq 1$ gilt

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

BEWEIS. Wegen Satz 1.2.6 gilt

$$\begin{aligned}\varphi(n) &= \sum_{k=1}^n \left\lfloor \frac{1}{(n, k)} \right\rfloor = \sum_{k=1}^n \sum_{d|(n, k)} \mu(d) = \sum_{k=1}^n \sum_{\substack{d|n \\ d|k}} \mu(d) \\ &= \sum_{d|n} \sum_{q=1}^{n/d} \mu(d) = \sum_{d|n} \mu(d) \left(\sum_{q=1}^{n/d} 1 \right) = \sum_{d|n} \mu(d) \frac{n}{d}.\end{aligned}$$

Hierbei schreibt man den Summationsindex k als $k = qd$ um (für festes $d \mid n$ müssen wir über solche $1 \leq k \leq n$ summieren, die Vielfache von d sind), wobei $1 \leq k \leq n$ genau dann gilt wenn $1 \leq q \leq \frac{n}{d}$. \square

SATZ 1.2.10. Für $n \geq 2$ gilt

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

BEWEIS. Es seien p_1, \dots, p_r die verschiedenen Primteiler von n . Dann ist

$$\begin{aligned}\prod_{p|n} \left(1 - \frac{1}{p}\right) &= \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) \\ &= 1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \sum \frac{1}{p_i p_j p_k} + \dots + \sum \frac{(-1)^r}{p_1 p_2 \dots p_r} \\ &= \sum_{d|n} \frac{\mu(d)}{d} \\ &= \frac{\varphi(n)}{n}.\end{aligned}$$

Hierbei bedeutet ein Summand wie zum Beispiel $\sum \frac{1}{p_i p_j}$, daß alle möglichen Produkte $p_i p_j$ von zwei verschiedenen Primteilern von n betrachtet werden. Jeder Summand ist von der Form $\frac{\mu(d)}{d}$, wobei d ein Teiler von n ist, der entweder 1 oder ein Produkt von verschiedenen Primzahlen ist. Wegen Satz 1.2.9 folgt die letzte Zeile. \square

Die Produktformel zeigt, wie gesagt, daß $\varphi(n)$ multiplikativ ist. Es folgen noch weitere Eigenschaften daraus:

SATZ 1.2.11. Die Eulersche φ -Funktion hat folgende Eigenschaften.

- (1) $\varphi(p^n) = p^n - p^{n-1}$, für $p \in \mathbb{P}$ und $n \geq 1$.
- (2) $\varphi(n^2) = n\varphi(n)$ für $n \geq 1$.
- (3) $\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$, wobei $d = (m, n)$.
- (4) $m \mid n \Rightarrow \varphi(m) \mid \varphi(n)$.
- (5) $\varphi(n)$ ist gerade für alle $n \geq 3$.

BEWEIS. Die Produktformel zeigt direkt $\varphi(p^n) = p^n(1 - \frac{1}{p}) = p^n - p^{n-1}$. Die zweite Eigenschaft folgt direkt aus (3). Um (3) zu zeigen, betrachte man

$$\frac{\varphi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Jeder Primteiler $p \mid mn$ teilt entweder m oder n . Diejenigen, die n und m teilen, teilen auch (m, n) . Das bedeutet

$$\begin{aligned} \frac{\varphi(mn)}{mn} &= \prod_{p|mn} \left(1 - \frac{1}{p}\right) = \frac{\prod_{p|m} \left(1 - \frac{1}{p}\right) \prod_{p|n} \left(1 - \frac{1}{p}\right)}{\prod_{p|(m,n)} \left(1 - \frac{1}{p}\right)} \\ &= \frac{\varphi(m)}{m} \cdot \frac{\varphi(n)}{n} \cdot \left(\frac{\varphi(d)}{d}\right)^{-1}, \end{aligned}$$

also die Behauptung. Für $d = (m, n) = 1$ folgt $\varphi(mn) = \varphi(m)\varphi(n)$, wie schon oben bemerkt. Zu (4): wegen $m \mid n$ gilt $n = mc$ mit $1 \leq c \leq n$. Für $c = n$ ist $m = 1$ und deshalb $\varphi(m) \mid \varphi(n)$ trivialerweise richtig. Sei also $c < n$. Wegen (3) folgt

$$\varphi(n) = \varphi(mc) = \varphi(m)\varphi(c) \frac{d}{\varphi(d)} = d\varphi(m) \frac{\varphi(c)}{\varphi(d)}$$

mit $d = (m, c)$. Wir beweisen damit (4) durch Induktion über n . Für $n = 1$ ist $m = c = 1$ und die Behauptung klar. Angenommen, (4) gilt für alle $1 \leq k < n$. Dann ist insbesondere $\varphi(d) \mid \varphi(c)$ wegen $d \mid c$. Also besagt obige Gleichung, daß $\varphi(n)$ ein ganzzahliges Vielfaches von $\varphi(m)$ ist, d.h., $\varphi(m) \mid \varphi(n)$.

Zu (5): für $n = 2^r$, $r \geq 2$ ist $\varphi(n) = 2^r - 2^{r-1}$ gerade. Hat n wenigstens einen ungeraden Primteiler, so folgt die Behauptung aus

$$\varphi(n) = n \prod_{p|n} \frac{p-1}{p} = \frac{n}{\prod_{p|n} p} \cdot \prod_{p|n} (p-1),$$

denn $\prod_{p|n} (p-1)$ ist dann gerade, und der Bruch ganzzahlig. Der Beweis zeigt noch mehr: jeder Primteiler $p > 2$ trägt einen Faktor 2 zu diesem Produkt bei. Deshalb folgt sogar

$$2^r \mid \varphi(n),$$

wobei n genau r verschiedene ungerade Primteiler hat. □

SATZ 1.2.12. Für $n \geq 1$ gilt

$$\sum_{d|n} \Lambda(d) = \log(n).$$

BEWEIS. Für $n = 1$ ist die Behauptung klar. Sei also $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \geq 2$. Logarithmieren ergibt $\log(n) = \sum_{i=1}^r \alpha_i \log(p_i)$. Nun kommen die von Null verschiedenen Terme in $\sum_{d|n} \Lambda(d)$ genau von solchen Teilern d , die von der Form p_i^m sind, mit $m = 1, 2, \dots, \alpha_i$ und $i = 1, 2, \dots, r$. Deshalb ist

$$\sum_{d|n} \Lambda(d) = \sum_{i=1}^r \sum_{m=1}^{\alpha_i} \Lambda(p_i^m) = \sum_{i=1}^r \sum_{m=1}^{\alpha_i} \log(p_i) = \sum_{i=1}^r \alpha_i \log(p_i) = \log(n).$$

□

DEFINITION 1.2.13. Die Liouvillesche λ -Funktion ist definiert durch

$$\lambda(n) = \begin{cases} 1 & \text{falls } n = 1, \\ (-1)^{\sum_{i=1}^r \alpha_i} & \text{falls } n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \geq 2. \end{cases}$$

Offensichtlich ist λ vollständig multiplikativ.

BEMERKUNG 1.2.14. Die arithmetischen Funktionen, die wir studiert haben, ergeben interessante Identitäten mit der Riemannschen Zetafunktion, wenn man mit ihnen Dirichlet-Reihen $\sum_{n=1}^{\infty} a_n n^{-s}$ bildet:

$$\begin{aligned} \sum_{n=1}^{\infty} \lambda(n) n^{-s} &= \frac{\zeta(2s)}{\zeta(s)}, \quad \sigma > 1 \\ \sum_{n=1}^{\infty} \mu(n) n^{-s} &= \frac{1}{\zeta(s)}, \quad \sigma > 1 \\ \sum_{n=1}^{\infty} \sigma_{\alpha}(n) n^{-s} &= \zeta(s) \zeta(s - \alpha), \quad \sigma > \max\{1, 1 + \operatorname{Re}(\alpha)\} \\ \sum_{n=1}^{\infty} \tau(n) n^{-s} &= \zeta(s)^2, \quad \sigma > 1 \\ \sum_{n=1}^{\infty} \varphi(n) n^{-s} &= \frac{\zeta(s-1)}{\zeta(s)}, \quad \sigma > 2 \\ \sum_{n=1}^{\infty} \Lambda(n) n^{-s} &= -\frac{\zeta'(s)}{\zeta(s)}, \quad \sigma > 1. \end{aligned}$$

1.3. Das Dirichlet-Produkt

Das Dirichlet-Produkt zweier arithmetischer Funktionen rührt von dem natürlichen Produkt zweier Dirichlet-Reihen her. Sei f eine arithmetische Funktion. Die *formale Dirichlet-Reihe* zu f ist definiert durch

$$D_f(s) = \sum_{n=1}^{\infty} f(n) n^{-s}.$$

Summe und Produkt sind in natürlicher Weise definiert. Mit

$$h(n) = \sum_{dd'=n} f(d)g(d')$$

haben wir

$$\begin{aligned} D_f(s) + D_g(s) &= \sum_{n=1}^{\infty} (f(n) + g(n)) n^{-s}, \\ D_f(s) D_g(s) &= \sum_{n=1}^{\infty} h(n) n^{-s}. \end{aligned}$$

Die Formel für das Produkt entsteht durch formales Ausmultiplizieren der Dirichlet-Reihen:

$$\begin{aligned} \sum_{m=1}^{\infty} f(m)m^{-s} \sum_{k=1}^{\infty} g(k)k^{-s} &= \sum_{m,k=1}^{\infty} f(m)g(k)(mk)^{-s} \\ &= \sum_{n=1}^{\infty} n^{-s} \left(\sum_{km=n} f(m)g(k) \right). \end{aligned}$$

Für zwei arithmetische Funktionen f, g werden nun arithmetische Funktionen $f + g, f * g$ so definiert, daß gilt

$$\begin{aligned} D_{f+g}(s) &= D_f(s) + D_g(s), \\ D_{f*g}(s) &= D_f(s)D_g(s). \end{aligned}$$

Das bedeutet folgendes:

DEFINITION 1.3.1. Für zwei arithmetische Funktionen f, g definiert man

$$\begin{aligned} (f + g)(n) &= f(n) + g(n), \\ (f * g)(n) &= \sum_{d|n} f\left(\frac{n}{d}\right)g(d) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right). \end{aligned}$$

Das Produkt heißt *Dirichlet-Produkt*, oder Dirichlet-Faltung.

Dieses Produkt ist kommutativ, wie man an der Darstellung

$$(f * g)(n) = \sum_{\substack{ab=n \\ a,b \in \mathbb{N}}} f(a)g(b)$$

sieht.

DEFINITION 1.3.2. Für $n \geq 1$ seien die arithmetischen Funktionen I, ε und id wie folgt definiert:

$$I(n) = \left\lfloor \frac{1}{n} \right\rfloor, \quad \varepsilon(n) = 1, \quad \text{id}(n) = n.$$

SATZ 1.3.3. Die arithmetischen Funktionen bilden mit der Addition und dem Dirichlet-Produkt einen faktoriellen Ring, also insbesondere einen Integritätsring. Wir bezeichnen ihn mit \mathcal{D} . Das Einselement bezüglich der Multiplikation ist durch I gegeben, d.h.,

$$I * f = f * I = f.$$

BEWEIS. Zunächst einmal zeigen wir, daß die Multiplikation assoziativ ist. Man hat

$$\begin{aligned} ((f * g) * h)(n) &= \sum_{\ell c=n} (f * g)(\ell) h(c) = \sum_{\ell c=n} h(c) \sum_{ab=\ell} f(a) g(b) \\ &= \sum_{abc=n} f(a) g(b) h(c), \\ (f * (g * h))(n) &= \sum_{ad=n} f(a) (g * h)(d) = \sum_{ad=n} f(a) \sum_{bc=d} g(b) h(c) \\ &= \sum_{abc=n} f(a) g(b) h(c). \end{aligned}$$

Des weiteren ist I ein Einselement, weil

$$(f * I)(n) = \sum_{d|n} f(d) I\left(\frac{n}{d}\right) = \sum_{d|n} f(d) \left\lfloor \frac{d}{n} \right\rfloor = f(n)$$

ist. In der Tat, $\left\lfloor \frac{d}{n} \right\rfloor = 0$ für $d < n$. Wegen der Kommutativität folgt $f = f * I = I * f$. Die weiteren Behauptungen können wir hier nicht beweisen. Man findet sie in [3]. \square

Wie sehen die Einheiten dieses Ringes aus, d.h., welche arithmetischen Funktionen sind invertierbar? Man findet, daß $f \in \mathcal{D}$ genau dann invertierbar ist, wenn $f(1) \neq 0$ ist.

SATZ 1.3.4. *Die Einheitengruppe des Ringes \mathcal{D} besteht aus den arithmetischen Funktionen f mit $f(1) \neq 0$. Für solche f kann man das Dirichlet-Inverse $g(n) = f^{-1}(n)$ rekursiv berechnen:*

$$\begin{aligned} g(1) &= f(1)^{-1} \\ g(n) &= -f(1)^{-1} \sum_{\substack{d|n \\ d < n}} f\left(\frac{n}{d}\right) g(d), \quad n \geq 2. \end{aligned}$$

BEWEIS. Die Gleichung $f * g = I$ ist ja äquivalent zu der Familie von Gleichungen, für jedes $n \geq 1$,

$$\sum_{d|n} f\left(\frac{n}{d}\right) g(d) = I(n).$$

Falls $f(1) = 0$ ist, so hat die Gleichung für $n = 1$ natürlich keine Lösung, und f ist nicht invertierbar. Andernfalls liefert obige Gleichung genau die angegebene Rekursionsformel. Man beachte, daß das Inverse eindeutig ist. Gälte neben $f * g = g * f = I$ auch noch $f * h = h * f = I$, so hätte man $f * h = f * g = I$ und somit

$$h = h * I = h * (f * g) = (h * f) * g = I * g = g.$$

\square

BEISPIEL 1.3.5. *Die μ -Funktion hat wegen $\mu(1) = 1$ ein Dirichlet-Inverses: es ist die ε -Funktion, d.h.,*

$$\mu * \varepsilon = \varepsilon * \mu = I.$$

In der Tat, Satz 1.2.6 besagt genau

$$(\varepsilon * \mu)(n) = \sum_{d|n} \mu(d) = I(n).$$

Mit Hilfe des Dirichlet-Produktes lassen sich unsere Resultate über Teilersummen nun ganz einfach formulieren:

$$\begin{aligned} n &= \sum_{d|n} \varphi(d) \iff \text{id} = \varepsilon * \varphi, \\ \varphi(n) &= \sum_{d|n} \mu(d) \frac{n}{d} \iff \varphi = \mu * \text{id}, \\ \log(n) &= \sum_{d|n} \Lambda(d) \iff \log = \Lambda * \varepsilon. \end{aligned}$$

Zudem kann man einige Sätze nun leichter beweisen. Aus $\varepsilon * \varphi = \text{id}$ folgt zum Beispiel $\varphi = \varepsilon^{-1} * \text{id} = \mu * \text{id}$, welches die zweite Identität (also Satz 1.2.9) beweist. Aus $\log = \Lambda * \varepsilon$ folgt $\Lambda = \log * \varepsilon^{-1} = \log * \mu$. Also ist die Λ -Funktion ein Produkt aus zwei bekannten arithmetischen Funktionen.

Multiplikative Funktionen sind übrigens Einheiten, da sie ja $f(1) = 1$ erfüllen. Sie bilden sogar eine Untergruppe.

SATZ 1.3.6. *Die Menge der multiplikativen arithmetischen Funktionen bildet eine Untergruppe der Einheitengruppe des Ringes \mathcal{D} .*

BEWEIS. Es seien f, g multiplikativ. Wir zeigen, daß dann auch $h := f * g$ multiplikativ ist. Es gelte $(m, n) = 1$. Dann haben wir nach Definition

$$h(mn) = \sum_{c|mn} f(c)g\left(\frac{mn}{c}\right).$$

Jeder Teiler $c \mid mn$ läßt sich aber in der Form $c = ab$, mit $a \mid m$ und $b \mid n$ schreiben. Wegen $(m, n) = 1$ ist

$$(a, b) = \left(\frac{m}{a}, \frac{n}{b}\right) = 1.$$

Man hat eine bijektive Korrespondenz zwischen der Menge der Produkte ab und den Teilern $c \mid mn$. Also folgt

$$\begin{aligned} h(mn) &= \sum_{\substack{a|m \\ b|n}} f(ab)g\left(\frac{mn}{ab}\right) = \sum_{\substack{a|m \\ b|n}} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) \\ &= \sum_{a|m} f(a)g\left(\frac{m}{a}\right) \cdot \sum_{b|n} f(b)g\left(\frac{n}{b}\right) = h(n)h(m). \end{aligned}$$

Entsprechend zeigt man auch, daß das Dirichlet-Inverse von f wieder multiplikativ ist. Für einen vollständigen Beweis des Satzes siehe [16] oder [1]. \square

BEISPIEL 1.3.7. *Da ε offensichtlich multiplikativ ist, und $\tau = \varepsilon * \varepsilon$, folgt erneut, daß die Teilerfunktion τ multiplikativ ist.*

In der Tat, es gilt

$$\tau(n) = \sum_{d|n} 1 = \sum_{d|n} \varepsilon(d) \varepsilon\left(\frac{n}{d}\right).$$

BEISPIEL 1.3.8. *Die Teilersummenfunktionen σ_k sind multiplikativ.*

Man hat für alle reellen oder komplexen Parameter k

$$\sigma_k(n) = \sum_{d|n} d^k = (j * \varepsilon)(n),$$

wobei $\varepsilon(n) = 1$ und $j(n) = n^k$ multiplikativ sind.

SATZ 1.3.9. *Ist f sogar streng multiplikativ, so ist das Dirichlet-Inverse von f durch $f^{-1} = \mu \cdot f$ gegeben, d.h., durch $f^{-1}(n) = \mu(n)f(n)$.*

BEWEIS. Wir schreiben $f \cdot g$ für diese Multiplikation, um sie von $f * g$ zu unterscheiden. Sei also $g = \mu \cdot f$. Dann gilt, da f streng multiplikativ ist,

$$(g * f)(n) = \sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right) = f(n) \sum_{d|n} \mu(d) = f(n)I(n) = I(n),$$

wegen Satz 1.2.6 und $f(1) = 1$, $I(n) = 0$ für $n \geq 2$. Das besagt genau $g * f = I$, oder $g = f^{-1}$. \square

BEISPIEL 1.3.10. *Das Dirichlet-Inverse der φ -Funktion ist durch $\varphi^{-1} = \varepsilon * (\mu \cdot \text{id})$ gegeben, d.h.,*

$$\varphi^{-1}(n) = \sum_{d|n} d\mu(d).$$

Wegen $\varphi = \mu * \text{id}$ ist $\varphi^{-1} = \text{id}^{-1} * \mu^{-1}$. Da id streng multiplikativ ist, folgt $\text{id}^{-1} = \mu \cdot \text{id}$ aus obigem Satz. Also gilt $\varphi^{-1} = \mu^{-1} * \mu \cdot \text{id} = \varepsilon * (\mu \cdot \text{id})$.

BEISPIEL 1.3.11. *Das Dirichlet-Inverse der λ -Funktion ist durch $\lambda^{-1}(n) = \mu(n)\lambda(n) = \mu^2(n) = |\mu(n)|$ gegeben.*

Das folgt wieder aus Satz 1.3.9, weil λ streng multiplikativ ist.

SATZ 1.3.12. *Ist f multiplikativ, so gilt*

$$\sum_{d|n} \mu(d)f(d) = \prod_{p|n} (1 - f(p)).$$

BEWEIS. Man setze

$$g(n) = \sum_{d|n} \mu(d)f(d).$$

Wegen Satz 1.3.6 ist g dann ebenfalls multiplikativ. Deshalb braucht man nur $g(p^\alpha)$ auszurechnen:

$$g(p^\alpha) = \sum_{d|p^\alpha} \mu(d)f(d) = \mu(1)f(1) + \mu(p)f(p) = 1 - f(p);$$

denn es ist $\mu(p^\alpha) = 0$ für $\alpha \geq 2$. \square

KOROLLAR 1.3.13. *Es gilt*

$$\varphi^{-1}(n) = \prod_{p|n} (1 - p).$$

BEWEIS. Wegen $\varphi^{-1}(n) = \sum_{d|n} d\mu(d)$ folgt das Korollar aus Satz 1.3.12 mit $f(d) = d$. \square

DEFINITION 1.3.14. Die *Dirichlet-Ableitung* f' einer arithmetischen Funktion f ist durch die arithmetische Funktion

$$f'(n) = f(n) \log(n)$$

gegeben.

Es ist zum Beispiel $I'(n) = 0$, weil $I(n) \log(n) = 0$ ist für $n \geq 1$. Weiterhin ist $\varepsilon'(n) = \log(n)$. Die Formel

$$\sum_{d|n} \Lambda(d) = \log(n)$$

kann man damit auch als $\Lambda * \varepsilon = \varepsilon'$ schreiben. Der Begriff Ableitung hat eine gewisse Berechtigung, wie der folgende Satz zeigt:

SATZ 1.3.15. *Für arithmetische Funktionen f, g gilt*

$$\begin{aligned} (f + g)' &= f' + g' \\ (f * g)' &= f' * g + f * g' \\ (f^{-1})' &= -f' * (f * f)^{-1}, \quad \text{falls } f(1) \neq 0. \end{aligned}$$

BEWEIS. Offenbar gilt

$$(f + g)'(n) = (f + g)(n) \log(n) = f(n) \log(n) + g(n) \log(n) = f'(n) + g'(n).$$

Die Derivationseigenschaft sieht man wie folgt: wegen $\log(n) = \log(d) + \log\left(\frac{n}{d}\right)$ gilt

$$\begin{aligned} (f * g)'(n) &= \sum_{d|n} f(d)g\left(\frac{n}{d}\right) \log(n) \\ &= \sum_{d|n} f(d) \log(d)g\left(\frac{n}{d}\right) + \sum_{d|n} f(d) \log\left(\frac{n}{d}\right)g\left(\frac{n}{d}\right) \\ &= (f' * g)(n) + (f * g')(n). \end{aligned}$$

Aus dieser Eigenschaft folgt

$$0 = I' = (f * f^{-1})' = f' * f^{-1} + f * (f^{-1})'.$$

Multipliziert man beide Seiten mit f^{-1} , so ergibt sich

$$\begin{aligned} 0 &= f^{-1} * f' * f^{-1} + (f^{-1})' \\ &= f' * f^{-1} * f^{-1} + (f^{-1})' \\ &= f' * (f * f)^{-1} + (f^{-1})'. \end{aligned}$$

\square

Als Anwendung der Dirichlet-Ableitung beweisen wir eine Formel von Selberg, die bei einem elementaren Beweis des Primzahlsatzes (durch Selberg und Erdős) Anwendung findet.

SATZ 1.3.16 (Selberg). Für $n \geq 1$ gilt

$$\Lambda(n) \log(n) + \sum_{d|n} \Lambda(d) \Lambda\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \log^2\left(\frac{n}{d}\right).$$

BEWEIS. Wir bilden die Dirichlet-Ableitung der oben erwähnten Identität $\Lambda * \varepsilon = \varepsilon'$. Das ergibt

$$\begin{aligned} \varepsilon'' &= (\Lambda * \varepsilon)' = \Lambda' * \varepsilon + \Lambda * \varepsilon' \\ &= \Lambda' * \varepsilon + \Lambda * (\Lambda * \varepsilon) \end{aligned}$$

Wegen $\varepsilon^{-1} = \mu$ folgt daraus

$$\varepsilon'' * \mu = \Lambda' + \Lambda * \Lambda.$$

Das zeigt die Behauptung. \square

BEMERKUNG 1.3.17. Wir haben noch nicht erwähnt, daß die Aussage des Primzahlsatzes

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

für $x \rightarrow \infty$ ist. Für den Beweis spielt die Λ -Funktion eine Rolle, beziehungsweise ihre summatorische Funktion

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

Denn der Primzahlsatz ist äquivalent zu der Aussage $\psi(x) \sim x$ für $x \rightarrow \infty$.

SATZ 1.3.18 (Erste Möbiussche Umkehrformel). Seien f, g arithmetische Funktionen. Dann sind folgende Eigenschaften äquivalent:

$$\begin{aligned} g(n) &= \sum_{d|n} f(d) \\ f(n) &= \sum_{d|n} g(d) \mu\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right). \end{aligned}$$

BEWEIS. Die erste Bedingung ist äquivalent zu $g = f * \varepsilon$; die zweite ist äquivalent zu $f = g * \mu$. Wegen $\mu^{-1} = \varepsilon$ folgt die Behauptung. \square

BEISPIEL 1.3.19. Für $n \geq 1$ gilt

$$\Lambda(n) = \sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right) = - \sum_{d|n} \mu(d) \log(d).$$

In Satz 1.2.12 haben wir $\log = \Lambda * \varepsilon$ gezeigt. Nach der Umkehrformel ist das äquivalent zu $\Lambda = \log * \mu$, wie wir auch schon früher gesehen haben. Schreibt man letzteres aus, so ergibt sich der erste Teil der Behauptung. Weiterhin ist

$$\begin{aligned} \sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right) &= \log(n) \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log(d) \\ &= \log(n) I(n) - \sum_{d|n} \mu(d) \log(d) \\ &= - \sum_{d|n} \mu(d) \log(d). \end{aligned}$$

Man kann das Dirichlet-Produkt noch wie folgt verallgemeinern.

DEFINITION 1.3.20. Sei F eine reell- oder komplexwertige Funktion, die auf $(0, \infty)$ definiert ist mit $F(x) = 0$ für $0 < x < 1$, und α eine arithmetische Funktion. Dann definiert man

$$(\alpha \circ F)(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right).$$

Ist $F(x) = 0$ für alle $x \notin \mathbb{Z}$, dann ist die Funktion $F|_{\mathbb{Z}}$ arithmetisch, und es gilt $(\alpha \circ F)(n) = (\alpha * F)(n)$. Allerdings ist die Operation \circ weder kommutativ noch assoziativ. Immerhin gilt (siehe [1] für einen Beweis):

SATZ 1.3.21. Für arithmetische Funktionen α, β gilt

$$\alpha \circ (\beta \circ F) = (\alpha * \beta) \circ F.$$

Man beachte, daß die Funktion I auch eine Linkseins bezüglich \circ ist.

SATZ 1.3.22 (Zweite Möbiussche Umkehrformel). Sei α eine Einheit des Ringes \mathcal{D} . Dann sind folgende Aussagen äquivalent:

$$\begin{aligned} G(x) &= \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right) \\ F(x) &= \sum_{n \leq x} \alpha^{-1}(n) G\left(\frac{x}{n}\right). \end{aligned}$$

Ist α streng multiplikativ, so ist dabei $\alpha^{-1}(n) = \mu(n)\alpha(n)$.

BEWEIS. Die erste Identität besagt $G = \alpha \circ F$, die zweite $F = \alpha^{-1} \circ G$. Aus der ersten folgt die zweite wie folgt:

$$\alpha^{-1} \circ G = \alpha^{-1} \circ (\alpha \circ F) = (\alpha^{-1} * \alpha) \circ F = I \circ F = F.$$

Die umgekehrte Richtung folgt analog. □

Natürlich ist die erste Möbiussche Umkehrformel ein Spezialfall der zweiten (man wähle $\alpha = \varepsilon$).

SATZ 1.3.23. Für $h = f * g$ setze man $H(x) = \sum_{n \leq x} h(n)$, $F(x) = \sum_{n \leq x} f(n)$ und $G(x) = \sum_{n \leq x} g(n)$. Dann gilt

$$H(x) = \sum_{n \leq x} f(n) G\left(\frac{x}{n}\right) = \sum_{n \leq x} g(n) F\left(\frac{x}{n}\right).$$

BEWEIS. Man definiere

$$U(x) = \begin{cases} 0 & \text{falls } 0 < x < 1, \\ 1 & \text{falls } x \geq 1. \end{cases}$$

Dann gilt $F = f \circ U$, $G = g \circ U$ und $H = h \circ U$. Mit Satz 1.3.21 gilt

$$\begin{aligned} f \circ G &= f \circ (g \circ U) = (f * g) \circ U = H, \\ g \circ F &= g \circ (f \circ U) = (g * f) \circ U = H. \end{aligned}$$

□

KOROLLAR 1.3.24. Mit $F(x) = \sum_{n \leq x} f(n)$ gilt

$$\sum_{n \leq x} \sum_{d|n} f(d) = \sum_{n \leq x} f(n) \left[\frac{x}{n} \right] = \sum_{n \leq x} F \left(\frac{x}{n} \right).$$

BEWEIS. Man wähle $g(n) = 1$ in obigem Satz, also $G(x) = [x]$. □

Als Anwendung dieses Korollars zeigen wir

SATZ 1.3.25. Für $x \geq 1$ gilt

$$\begin{aligned} \sum_{n \leq x} \mu(n) \left[\frac{x}{n} \right] &= 1, \\ \sum_{n \leq x} \Lambda(n) \left[\frac{x}{n} \right] &= \log([x!]). \end{aligned}$$

BEWEIS. Wir wenden das Korollar mit $f(n) = \mu(n)$ bzw. $f(n) = \Lambda(n)$ an. Dann erhalten wir

$$\begin{aligned} \sum_{n \leq x} \mu(n) \left[\frac{x}{n} \right] &= \sum_{n \leq x} \sum_{d|n} \mu(d) = \sum_{n \leq x} \left[\frac{1}{n} \right] = 1, \\ \sum_{n \leq x} \Lambda(n) \left[\frac{x}{n} \right] &= \sum_{n \leq x} \sum_{d|n} \Lambda(d) = \sum_{n \leq x} \log n = \log([x!]). \end{aligned}$$

□

BEMERKUNG 1.3.26. Die Aussage über das gewichtete Mittel der μ -Funktion legt vielleicht die Vermutung nahe, daß gilt

$$\lim_{x \rightarrow \infty} \sum_{n \leq x} \frac{\mu(n)}{n} = 0.$$

Diese Aussage ist in der Tat äquivalent zum Primzahlsatz.

KOROLLAR 1.3.27. Für jedes $x \geq 1$ gilt

$$[x!] = \prod_{p \leq x} p^{\alpha(p)}, \quad \text{mit } \alpha(p) = \sum_{m=1}^{\infty} \left[\frac{x}{p^m} \right].$$

BEWEIS. Zunächst beachte man, daß die Summe für $\alpha(p)$ endlich ist, da $[x/p^m] = 0$ für $p > x$. Mit der Identität für Λ aus Satz 1.3.25 folgt

$$\log([x!]) = \sum_{n \leq x} \Lambda(n) \left[\frac{x}{n} \right] = \sum_{p \leq x} \sum_{m=1}^{\infty} \left[\frac{x}{p^m} \right] \log(p) = \sum_{p \leq x} \alpha(p) \log(p).$$

Hierbei haben wir benutzt, daß nur für $n = p^m$ die Terme $\Lambda(n) = \Lambda(p^m) = \log(p)$ von Null verschieden sind, und aus $p^m \leq x$ folgt $p \leq x$. □

1.4. Die Eulersche Summationsformel

Manchmal kann man den asymptotischen Wert einer Summe bestimmen, indem man sie mit einem Integral vergleicht. Die Summationsformel von Euler gibt den genauen Fehler an, der bei einer solchen Approximation entsteht.

SATZ 1.4.1 (Eulersche Summationsformel). *Sei f eine reelle Funktion der Klasse C^1 auf dem Interval $[y, x]$, $0 < y < x$, d.h., f' ist auf $[y, x]$ stetig. Dann gilt*

$$\sum_{y < n \leq x} f(n) = \int_y^x f(t) dt + \int_y^x (t - [t]) f'(t) dt \\ + f(x)([x] - x) - f(y)([y] - y).$$

Dieser Satz ist ein Spezialfall der sogenannten Abelschen Summation:

SATZ 1.4.2. *Sei $a(n)$ eine arithmetische Funktion, und*

$$A(x) = \begin{cases} \sum_{n \leq x} a(n) & \text{für } x \geq 1, \\ 0 & \text{für } x < 1. \end{cases}$$

Sei $f \in C^1([y, x])$ für $0 < y < x$. Dann gilt

$$\sum_{y < n \leq x} a(n) f(n) = A(x) f(x) - A(y) f(y) - \int_y^x A(t) f'(t) dt.$$

BEWEIS. Zunächst beachte man, daß $A(t)$ auf $[n, n + 1)$ konstant ist. Seien $k = [x]$ und $m = [y]$. Dann gilt $A(x) = A(k)$ und $A(y) = A(m)$. Da $A(t)$ konstant ist auf $[k, x]$, folgt

$$A(x) f(x) - \int_k^x A(t) f'(t) dt = A(x) f(x) - A(x) \int_k^x f'(t) dt \\ = A(x) f(x) - A(x) (f(x) - f(k)) = A(k) f(k).$$

Ebenso folgt

$$A(y) f(y) - \int_{m+1}^y A(t) f'(t) dt = A(m) f(m + 1).$$

Mit $A(n) - A(n - 1) = a(n)$ und diesen beiden Formeln (die man benutzt, um $A(k)f(k)$ und $A(m)f(m + 1)$ zu ersetzen) folgt:

$$\begin{aligned}
\sum_{y < n \leq x} a(n)f(n) &= \sum_{n=m+1}^k a(n)f(n) = \sum_{n=m+1}^k (A(n) - A(n - 1))f(n) \\
&= \sum_{n=m+1}^k A(n)f(n) - \sum_{n=m}^{k-1} A(n)f(n + 1) \\
&= A(k)f(k) - A(m)f(m + 1) + \sum_{n=m+1}^{k-1} A(n)(f(n) - f(n + 1)) \\
&= A(k)f(k) - A(m)f(m + 1) - \sum_{n=m+1}^{k-1} A(n) \int_n^{n+1} f'(t) dt \\
&= A(k)f(k) - A(m)f(m + 1) - \sum_{n=m+1}^{k-1} \int_n^{n+1} A(t)f'(t) dt \\
&= A(k)f(k) - A(m)f(m + 1) - \int_{m+1}^k A(t)f'(t) dt \\
&= A(x)f(x) - A(y)f(y) - \int_y^{m+1} A(t)f'(t) dt \\
&\quad - \int_{m+1}^k A(t)f'(t) dt - \int_k^x A(t)f'(t) dt \\
&= A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t) dt.
\end{aligned}$$

□

Für $y < 1$ ist $A(y) = 0$. Dann folgt das folgende Korollar.

KOROLLAR 1.4.3. Für $x \geq 1$ folgt

$$\sum_{n \leq x} a(n)f(n) = A(x)f(x) - \int_1^x A(t)f'(t) dt.$$

Beweis von Satz 1.4.1: Man wähle $a(n) = 1$ für $n \geq 1$, so daß $A(x) = [x]$ ist. Dann liefert die Abelsche Summationsformel

$$\sum_{y < n \leq x} f(n) = f(x)[x] - f(y)[y] - \int_y^x [t]f'(t) dt.$$

Kombiniert man das mit der Formel für partielle Integration

$$\int_y^x t f'(t) dt = x f(x) - y f(y) - \int_y^x f(t) dt,$$

so folgt die Behauptung. □

Die Summationsformeln haben viele Anwendungen.

SATZ 1.4.4. Für $\alpha, \sigma \in \mathbb{R}$ und $x \geq 1$ gelten folgende Aussagen:

$$\begin{aligned}\sum_{n \leq x} \frac{1}{n} &= \log(x) + \gamma + O\left(\frac{1}{x}\right), \\ \sum_{n \leq x} \frac{1}{n^\sigma} &= \frac{x^{1-\sigma}}{1-\sigma} + \zeta(\sigma) + O(x^{-\sigma}), \quad \sigma \neq 1, \sigma > 0 \\ \sum_{n > x} \frac{1}{n^\sigma} &= O(x^{1-\sigma}), \quad \sigma > 1 \\ \sum_{n \leq x} n^\alpha &= \frac{x^{\alpha+1}}{\alpha+1} + O(x^\alpha), \quad \alpha \geq 0.\end{aligned}$$

BEWEIS. Für die erste Aussage wähle man in der Eulerschen Summationsformel $f(t) = \frac{1}{t}$ und $y = 1$. Dann liefert sie, mit $f'(t) = -\frac{1}{t^2}$,

$$\begin{aligned}\sum_{n \leq x} \frac{1}{n} &= 1 + \sum_{1 < n \leq x} \frac{1}{n} = 1 + \int_1^x \frac{dt}{t} + \int_1^x \frac{t - [t]}{-t^2} dt + \frac{[x] - x}{x} - 0 \\ &= \log(x) + 1 - \int_1^x \frac{t - [t]}{t^2} dt + O\left(\frac{1}{x}\right) \\ &= \log(x) + \left(1 - \int_1^\infty \frac{t - [t]}{t^2} dt\right) + \int_x^\infty \frac{t - [t]}{t^2} dt + O\left(\frac{1}{x}\right).\end{aligned}$$

Dabei ist $1 - \int_1^\infty \frac{t - [t]}{t^2} dt$ eine Konstante, weil das Integral existiert: es wird durch $\int_1^\infty t^{-2} dt$ dominiert. Das letzte Integral verschwindet in dem O -Term wegen

$$0 \leq \int_x^\infty \frac{t - [t]}{t^2} dt \leq \int_x^\infty t^{-2} dt = \frac{1}{x}.$$

Für $x \rightarrow \infty$ erhält man daraus dann

$$\gamma = \lim_{x \rightarrow \infty} \left(\sum_{n \leq x} \frac{1}{n} - \log(x) \right) = 1 - \int_1^\infty \frac{t - [t]}{t^2} dt.$$

Damit ist die erste Aussage vollständig gezeigt.

Für die zweite Aussage wähle man $f(t) = t^{-\sigma}$ mit $f'(t) = -\sigma t^{-\sigma-1}$, $y = 1$ und wende die ESF an. Dann erhält man

$$\sum_{n \leq x} \frac{1}{n^\sigma} = \int_1^x \frac{dt}{t^\sigma} - \sigma \int_1^x \frac{t - [t]}{t^{\sigma+1}} dt + \frac{[x] - x}{x^\sigma} + 1.$$

Wie oben ersetzt man die obere Grenze des zweiten Integrals durch unendlich, wobei man den Fehler

$$\sigma \int_x^\infty \frac{t - [t]}{t^{\sigma+1}} dt = O(x^{-\sigma})$$

macht. Es folgt

$$\begin{aligned}\sum_{n \leq x} \frac{1}{n^\sigma} &= \frac{x^{1-\sigma}}{1-\sigma} - \frac{1}{1-\sigma} + 1 - \sigma \int_1^\infty \frac{t - [t]}{t^{\sigma+1}} dt + O(x^{-\sigma}) \\ &= \frac{x^{1-\sigma}}{1-\sigma} + C(\sigma) + O(x^{-\sigma}),\end{aligned}$$

wobei

$$C(\sigma) = 1 - \frac{1}{1-\sigma} - \sigma \int_1^\infty \frac{t - [t]}{t^{\sigma+1}} dt.$$

Für $\sigma > 1$ betrachtet man nun, was für $x \rightarrow \infty$ passiert. Die linke Seite geht gegen $\zeta(\sigma)$, während die Terme $x^{1-\sigma}$ und $x^{-\sigma}$ beide gegen Null gehen. Also folgt

$$C(\sigma) = \zeta(\sigma), \quad \sigma > 1.$$

Für $0 < \sigma < 1$ hat man auch $x^{-\sigma} \rightarrow 0$ für $x \rightarrow \infty$ und $C(\sigma) = \zeta(\sigma)$, da man ja $\zeta(\sigma)$ in diesem Streifen genau durch

$$\lim_{x \rightarrow \infty} \left(\sum_{n \leq x} n^{-\sigma} - \frac{x^{1-\sigma}}{1-\sigma} \right) = C(\sigma)$$

fortsetzt. Das zeigt die zweite Behauptung. Aus ihr folgt für $\sigma > 1$ dann auch

$$\sum_{n > x} \frac{1}{n^\sigma} = \zeta(\sigma) - \sum_{n \leq x} \frac{1}{n^\sigma} = \frac{x^{1-\sigma}}{\sigma-1} + O(x^{-\sigma}) = O(x^{1-\sigma}),$$

weil $x^{-\sigma} \leq x^{1-\sigma}$ für $\sigma > 1$ gilt. Damit folgt die dritte Aussage.

Zum Schluß wählen wir $f(t) = t^\alpha$ mit $f'(t) = \alpha t^{\alpha-1}$. Es folgt

$$\begin{aligned}\sum_{n \leq x} n^\alpha &= \int_1^x t^\alpha dt + \alpha \int_1^x t^{\alpha-1} (t - [t]) dt + 1 - (x - [x])x^\alpha \\ &= \frac{x^{\alpha+1}}{\alpha+1} - \frac{1}{\alpha+1} + O\left(\alpha \int_1^x t^{\alpha-1} dt\right) + O(x^\alpha) \\ &= \frac{x^{\alpha+1}}{\alpha+1} + O(x^\alpha).\end{aligned}$$

□

SATZ 1.4.5. Für $x \geq 2$ gilt

$$\sum_{n \leq x} \Lambda(n) \left[\frac{x}{n} \right] = \log([x]!) = x \log(x) - x + O(\log(x)).$$

BEWEIS. Der erste Teil folgt aus Satz 1.3.25. Für den zweiten Teil wählen wir $f(t) = \log(t)$ in der ESF und erhalten

$$\begin{aligned}
\sum_{n \leq x} \log(n) &= \int_1^x \log(t) dt + \int_1^x \frac{t - [t]}{t} dt + ([x] - x) \log(x) \\
&= x \log(x) - x + 1 + \int_1^x \frac{t - [t]}{t} dt + O(\log(x)) \\
&= x \log(x) - x + O(\log(x)).
\end{aligned}$$

Im letzten Schritt haben wir benutzt, daß das Integral gleich

$$O\left(\int_1^x \frac{1}{t} dt\right) = O(\log(x))$$

ist. □

KOROLLAR 1.4.6. Für $x \geq 2$ gilt

$$\sum_{p \leq x} \left[\frac{x}{p} \right] \log(p) = x \log(x) + O(x).$$

BEWEIS. Wie in Korollar 1.3.27 haben wir

$$\sum_{n \leq x} \Lambda(n) \left[\frac{x}{n} \right] = \sum_{p \leq x} \sum_{m=1}^{\infty} \left[\frac{x}{p^m} \right] \log(p) = \sum_{p \leq x} \left[\frac{x}{p} \right] \log(p) + \sum_{p \leq x} \sum_{m=2}^{\infty} \left[\frac{x}{p^m} \right] \log(p).$$

Wenn wir zeigen können, daß die letzte Summe ein $O(x)$ ist, folgt die Behauptung zusammen mit Satz 1.4.5. Wir schätzen die Summe wie folgt ab:

$$\begin{aligned}
\sum_{p \leq x} \sum_{m=2}^{\infty} \left[\frac{x}{p^m} \right] \log(p) &\leq \sum_{p \leq x} \log(p) \sum_{m=2}^{\infty} \frac{x}{p^m} = x \sum_{p \leq x} \log(p) \sum_{m=2}^{\infty} p^{-m} \\
&= x \sum_{p \leq x} \log(p) \cdot \frac{1}{p^2} \left(1 - \frac{1}{p}\right)^{-1} \\
&= x \sum_{p \leq x} \frac{\log(p)}{p(p-1)} \leq x \sum_{n=2}^{\infty} \frac{\log(n)}{n(n-1)} = O(x),
\end{aligned}$$

denn die letzte Reihe ist beschränkt. □

BEMERKUNG 1.4.7. In der Tat gilt

$$\sum_{n=2}^{\infty} \frac{\log(n)}{n(n-1)} \leq \sum_{r=1}^{\infty} \sum_{\substack{2^{r-1} < n \\ 2^r \geq n}} \frac{r \log(2)}{n(n-1)} = \sum_{r=1}^{\infty} \frac{r \log(2)}{2^r} = \log(4).$$

1.5. Ein Taubersatz von Shapiro

Wir beweisen hier einen Satz von H.N. Shapiro, der Summen der Form $\sum_{n \leq x} a(n)$ mit Summen $\sum_{n \leq x} a(n)[x/n]$ in Verbindung bringt, siehe [15]. Als Anwendung erhalten wir zwei Theoreme von Mertens.

THEOREM 1.5.1 (Shapiro). *Es sei $(a(n))$ eine Folge nicht-negativer reeller Zahlen, so daß für $x \geq 1$ gilt*

$$\sum_{n \leq x} a(n) \left[\frac{x}{n} \right] = x \log(x) + O(x).$$

Dann gelten folgende Aussagen:

- (1) $\sum_{n \leq x} \frac{a(n)}{n} = \log(x) + O(1)$ für $x \geq 1$.
- (2) $\sum_{n \leq x} a(n) \leq Bx$ für $x \geq 1$ und eine Konstante $B > 0$.
- (3) $\sum_{n \leq x} a(n) \geq Ax$ für $x \geq x_0$ und ein $x_0 > 1$, sowie eine Konstante $A > 0$.

BEWEIS. Zur Abkürzung setzen wir

$$S(x) = \sum_{n \leq x} a(n), \quad T(x) = \sum_{n \leq x} a(n) \left[\frac{x}{n} \right], \quad A(x) = \sum_{n \leq x} \frac{a(n)}{n}.$$

Wir zeigen zuerst, für $x \geq 1$, die Ungleichung

$$(1.3) \quad S(x) - S\left(\frac{x}{2}\right) \leq T(x) - 2T\left(\frac{x}{2}\right).$$

Da für $y \geq 0$ gilt $[2y] - 2[y] \geq 0$, nämlich 0 oder 1, folgt

$$\begin{aligned} T(x) - 2T\left(\frac{x}{2}\right) &= \sum_{n \leq x} a(n) \left[\frac{x}{n} \right] - 2 \sum_{n \leq x/2} a(n) \left[\frac{x}{2n} \right] \\ &= \sum_{n \leq x/2} a(n) \left(\left[\frac{x}{n} \right] - 2 \left[\frac{x}{2n} \right] \right) + \sum_{x/2 < n \leq x} a(n) \left[\frac{x}{n} \right] \\ &\geq \sum_{x/2 < n \leq x} a(n) \left[\frac{x}{n} \right] = \sum_{x/2 < n \leq x} a(n) = S(x) - S\left(\frac{x}{2}\right), \end{aligned}$$

weil $[x/n] = 1$ für $x/2 < n \leq x$ gilt. Damit beweisen wir jetzt (2). Nach Voraussetzung ist $T(x) = x \log(x) + O(x)$. Also folgt

$$\begin{aligned} T(x) - 2T\left(\frac{x}{2}\right) &= x \log(x) - 2 \cdot \frac{x}{2} \log\left(\frac{x}{2}\right) + O(x) \\ &= O(x). \end{aligned}$$

Wegen (1.3) folgt daraus auch $S(x) - S\left(\frac{x}{2}\right) = O(x)$. Es gibt also eine Konstante $c > 0$ mit

$$S(x) - S\left(\frac{x}{2}\right) \leq cx, \quad x \geq 1.$$

Man ersetze x hierin sukzessive durch $\frac{x}{2}, \frac{x}{4}, \dots, \frac{x}{2^{n-1}}$ mit $2^n > x$. Wir haben $S\left(\frac{x}{2^n}\right) = 0$, weil dann das Argument kleiner als Eins ist. Damit erhalten wir die Ungleichungen

$$\begin{aligned} S(x) - S\left(\frac{x}{2}\right) &\leq cx \\ S\left(\frac{x}{2}\right) - S\left(\frac{x}{4}\right) &\leq c\frac{x}{2} \\ &\vdots \leq \vdots \\ S\left(\frac{x}{2^{n-1}}\right) - S\left(\frac{x}{2^n}\right) &\leq c\frac{x}{2^{n-1}}. \end{aligned}$$

Addiert man alle Ungleichungen, so folgt

$$S(x) - 0 \leq cx \left(1 + \frac{1}{2} + \dots + \frac{1}{2^{n-1}}\right) < 2cx.$$

Mit $B := 2c$ folgt also $\sum_{n \leq x} a(n) = S(x) \leq Bx$.

Jetzt zeigen wir (1). Wenn wir $[x/n] = x/n + O(1)$ schreiben, folgt mit (2)

$$\begin{aligned} T(x) &= \sum_{n \leq x} a(n) \left[\frac{x}{n}\right] = \sum_{n \leq x} \left(\frac{x}{n} + O(1)\right) a(n) \\ &= x \sum_{n \leq x} \frac{a(n)}{n} + O\left(\sum_{n \leq x} a(n)\right) = x \sum_{n \leq x} \frac{a(n)}{n} + O(x). \end{aligned}$$

Also folgt, mit der Voraussetzung,

$$\sum_{n \leq x} \frac{a(n)}{n} = \frac{1}{x} T(x) + O(1) = \frac{x \log(x)}{x} + O(1) = \log(x) + O(1).$$

Um schließlich (3) zu zeigen, schreiben wir (1) als $A(x) = \log(x) + R(x)$ mit einem Fehlerterm $R(x)$, der $|R(x)| \leq M$ für eine Konstante $M > 0$ erfüllt. Für $x \geq 1$ und $0 < \alpha < 1$ mit $\alpha x \geq 1$ folgt

$$\begin{aligned} A(x) - A(\alpha x) &= \log(x) + R(x) - \log(\alpha x) - R(\alpha x) \\ &= -\log(\alpha) + R(x) - R(\alpha x) \\ &\geq -\log(\alpha) - |R(x)| - |R(\alpha x)| \geq -\log(\alpha) - 2M. \end{aligned}$$

Nun wähle hier $\alpha = \exp(-2M-1)$. Dann folgt $\log(\alpha) = -2M-1$ und deshalb $-\log(\alpha) - 2M = 1$. Damit hat man also

$$A(x) - A(\alpha x) \geq 1, \quad x \geq \frac{1}{\alpha},$$

$$A(x) - A(\alpha x) = \sum_{\alpha x < n \leq x} \frac{a(n)}{n} \leq \frac{1}{\alpha x} \sum_{n \leq x} a(n) = \frac{S(x)}{\alpha x}.$$

Es folgt $S(x) \geq \alpha x$ für $x \geq \frac{1}{\alpha}$. Das zeigt (3) mit $A = \alpha$ und $x_0 = 1/\alpha$. □

SATZ 1.5.2 (Mertens 1). *Für alle $x \geq 1$ gilt*

$$\sum_{p \leq x} \frac{\log(p)}{p} = \log(x) + O(1).$$

BEWEIS. Wir wählen in Shapiros Satz

$$a(n) = \begin{cases} \log(p) & \text{falls } p \in \mathbb{P}, \\ 0 & \text{sonst.} \end{cases}$$

Es gilt $a(n) \geq 0$. Nun sind die Voraussetzungen in Shapiros Satz erfüllt, weil mit Korollar 1.4.6 folgt

$$\sum_{n \leq x} a(n) \left[\frac{x}{n} \right] = \sum_{p \leq x} \left[\frac{x}{p} \right] \log(p) = x \log(x) + O(x).$$

Shapiros Satz (1) liefert also:

$$\sum_{p \leq x} \frac{\log(p)}{p} = \sum_{n \leq x} \frac{a(n)}{n} = \log(x) + O(1).$$

□

SATZ 1.5.3 (Mertens 2). *Für alle $x \geq 1$ gilt*

$$\sum_{n \leq x} \frac{\Lambda(n)}{n} = \log(x) + O(1).$$

BEWEIS. Wir wählen $a(n) = \Lambda(n) \geq 0$ in Shapiros Satz. Wegen Satz 1.4.5 ist die Voraussetzung erfüllt:

$$\sum_{n \leq x} \frac{a(n)}{n} = \sum_{n \leq x} \frac{\Lambda(n)}{n} = x \log(x) + O(x).$$

Die Behauptung folgt also wieder aus (1) in Shapiros Satz. □

BEMERKUNG 1.5.4. Der dritte Satz von Mertens besagt, für $x \geq 2$,

$$\sum_{p \leq x} \frac{1}{p} = \log(\log(x)) + c + O\left(\frac{1}{\log x}\right),$$

siehe Bemerkung 1.1.14. Es existiert auch noch eine Mertens-Formel. Sie besagt, für $x \geq 2$,

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log(x)} \left(1 + O\left(\frac{1}{\log x}\right)\right).$$

Für einen Beweis siehe zum Beispiel [16], I.1.6. In diesem Zusammenhang kann man auch noch die Mertens-Vermutung erwähnen. Sie besagte, für $x > 1$,

$$\left| \sum_{n \leq x} \mu(n) \right| = |M(x)| < \sqrt{x}.$$

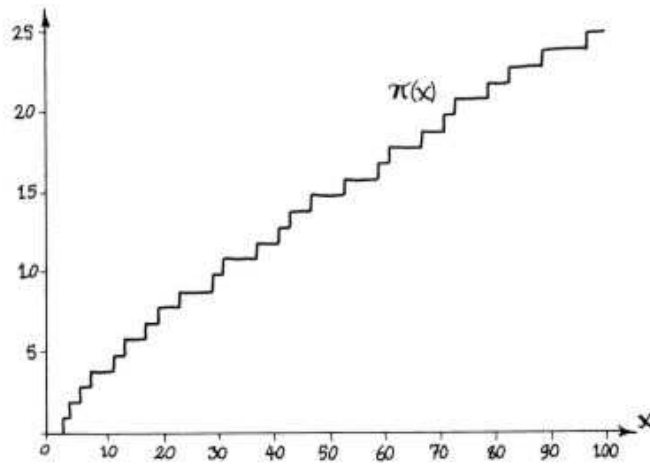
Diese Vermutung gilt für alle $x \leq 10^{13}$, so daß man glauben könnte, sie sei immer richtig. Doch das ist nicht wahr. Die Ungleichung ist unendlich oft falsch, siehe [14]. Ein explizites Gegenbeispiel ist allerdings noch nicht bekannt. Die Mertensche Vermutung hätte übrigens die Riemannsche Vermutung impliziert.

1.6. Über die Primzahlverteilung

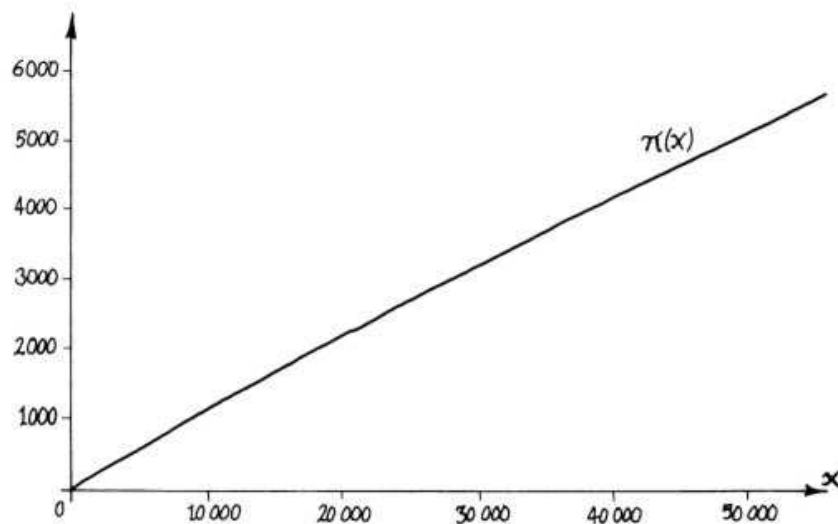
Die Primzahlverteilung ist lokal gesehen sehr irregulär. Es gibt keinen offensichtlichen Grund, warum die eine Zahl prim ist, und die andere nicht: wieso sind im Intervall $[10000000, 10000100]$ genau die beiden Zahlen

$$10000019, 10000079$$

prim und die anderen nicht? Der folgende Graph zeigt, wie irregulär die Werte der Funktion $\pi(x)$ im Intervall $[1, 100]$ sind:



Schaut man jedoch global auf die Primzahlverteilung, so ändert sich das Bild:



Don Zagier schreibt in einem Aufsatz über die ersten 50 Millionen Primzahlen: "For me, the smoothness with which this curve climbs is one of the most astonishing facts in mathematics." Gauß studierte als 15-jähriger schon stundenlang Primzahltabellen. Er kam bereits 1792 zu der Vermutung

$$\pi(x) \sim \int_2^x \frac{dt}{\log(t)}.$$

Das auftretende Integral heißt Integrallogarithmus, und es gilt

$$\operatorname{li}(x) = \int_2^x \frac{dt}{\log(t)} = \frac{x}{\log(x)} + O\left(\frac{x}{\log^2(x)}\right).$$

Legendre veröffentlichte die Vermutung $\pi(x) \sim x/\log(x)$ dann 1798. Ein Beweis wurde aber erst sehr viel später gegeben, nämlich 1896 von Hadamard, und unabhängig davon, von de la Vallée Poussin:

THEOREM 1.6.1 (PNT). *Für $x \rightarrow \infty$ gilt*

$$\pi(x) \sim \frac{x}{\log(x)} \sim \operatorname{li}(x).$$

Man sollte dazu noch sagen, daß $\operatorname{li}(x)$ die deutlich bessere Approximation von $\pi(x)$ ist. Es ist leicht zu zeigen, daß *wenn* der Grenzwert

$$\lim_{x \rightarrow \infty} \pi(x) \frac{\log(x)}{x}$$

existiert, daß er dann gleich 1 sein muß. Die Schwierigkeit liegt darin, daß überhaupt der Grenzwert existiert. Dafür gibt es bis heute keinen einfachen Beweis. Die kürzesten Beweise beruhen alle auf den analytischen Eigenschaften von $\zeta(s)$ mithilfe komplexer Analysis. Riemann hatte 1859 diese Idee gegeben. Für einen relativen kurzen Beweis des PNT siehe [17]. Es gibt auch Beweise, die ohne diese komplexe Analysis auskommen. Sie sind aber keineswegs einfacher. Die folgende Tabelle soll den PNT numerisch illustrieren. Die Zahlen für $\operatorname{li}(x)$ sind in Wirklichkeit $[\operatorname{li}(x)]$. Für $x = 10^{10}$ ist zum Beispiel $\pi(x) = 455052511$ und

$$[\operatorname{li}(x)] = 455055614, \quad \left[\frac{x}{\log(x)} \right] = 434294482.$$

x	$\pi(x)$	$\operatorname{li}(x)$
10^1	4	5
10^2	25	29
10^3	168	177
10^4	1229	1245
10^5	9592	9629
10^6	78498	78627
10^7	664579	664917
10^8	5761455	5762208
10^9	50847534	50849234
10^{10}	455052511	455055614
10^{11}	4118054813	4118066400
10^{12}	37607912018	37607950280

Es scheint, als ob immer $\text{li}(x) - \pi(x) > 0$ gelten würde. Erstaunlicherweise ist das falsch:

THEOREM 1.6.2 (Littlewood, 1914). *Es gibt unendlich viele Werte von x für die $\pi(x) > \text{li}(x)$ gilt.*

Die Frage ist dann, was das kleinste x_1 ist mit $\pi(x_1) > \text{li}(x_1)$. Dafür gibt es nur gigantisch große Abschätzungen. Die beste bisher, von Bays und Hudson (1999), besagt

$$x_1 < 1.3982 \cdot 10^{316}.$$

In der Tat führen Bays und Hudson plausible Gründe dafür an, daß x_1 tatsächlich in dieser Größenordnung liegen sollte.

Riemann fand dagegen eine exakte Formel für $\pi(x)$. Er betrachtete

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

Die Reihe konvergiert sehr schnell, und Riemann fand die Formel

$$\pi(x) = R(x) - \sum_{\rho \in \mathcal{N}} R(x^\rho),$$

wobei die Summe über die Nullstellen von $\zeta(s)$ läuft. Da die Summe über die Nullstellen nicht absolut konvergent ist, muß man in der richtigen Reihenfolge aufsummieren, nämlich nach wachsendem Absolutbetrag von $\text{Im}(\rho)$. Die Formel wurde 1895 von Mangoldt bewiesen. $\zeta(s)$ hat sogenannte triviale Nullstellen bei $\rho = -2, -4, -6, \dots$. Die anderen sind bis heute ein Mysterium. Die vielleicht wichtigste ungelöste Vermutung der Zahlentheorie ist:

VERMUTUNG 1.6.3 (Riemann). *Die Zetafunktion $\zeta(s)$ hat im Streifen $0 < \text{Re}(s) < 1$ keine Nullstelle außerhalb der kritischen Geraden $\text{Re}(s) = \frac{1}{2}$.*

Die ersten Nullstellen sind

$$\rho_1 = \frac{1}{2} + 14.134725i$$

$$\rho_2 = \frac{1}{2} + 21.022040i$$

$$\rho_3 = \frac{1}{2} + 25.010856i$$

$$\rho_4 = \frac{1}{2} + 30.424878i$$

$$\rho_5 = \frac{1}{2} + 32.9345057i.$$

Mit ρ tritt auch $\bar{\rho}$ auf. Die Riemannsche Vermutung ist äquivalent zu der Aussage, daß es für jedes $\varepsilon > 0$ eine Konstante $C_\varepsilon > 0$ gibt mit

$$|\pi(x) - \text{li}(x)| \leq C_\varepsilon x^{\frac{1}{2} + \varepsilon}.$$

Wir kommen nun zu elementarerem Resultaten der Primzahlverteilung zurück. Wir können hier mit wenig Aufwand die folgenden Ungleichungen zeigen:

SATZ 1.6.4. Für jedes $n \geq 2$ gilt

$$\frac{1}{6} \frac{n}{\log(n)} < \pi(n) < 6 \frac{n}{\log(n)}.$$

BEWEIS. Wir beginnen mit den Ungleichungen

$$(1.4) \quad 2^n \leq \binom{2n}{n} < 4^n.$$

Die linke Seite folgt mit Induktion, die rechte wie folgt:

$$4^n = (1+1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} > \binom{2n}{n}.$$

Logarithmiert man nun (1.4), so folgt

$$(1.5) \quad n \log(2) \leq \log(2n!) - 2 \log(n!) < n \log(4).$$

Aus dem Beweis von Korollar 1.3.27 wissen wir aber, daß

$$\log(n!) = \sum_{p \leq n} \alpha(p) \log(p), \quad \text{mit } \alpha(p) = \sum_{m=1}^{\left\lfloor \frac{\log(n)}{\log(p)} \right\rfloor} \left\lfloor \frac{n}{p^m} \right\rfloor.$$

Deshalb folgt

$$(1.6) \quad \log(2n!) - 2 \log(n!) = \sum_{p \leq 2n} \sum_{m=1}^{\left\lfloor \frac{\log(2n)}{\log(p)} \right\rfloor} \left(\left\lfloor \frac{2n}{p^m} \right\rfloor - 2 \left\lfloor \frac{n}{p^m} \right\rfloor \right) \log(p).$$

Da aber $[2x] - 2[x]$ entweder 0 oder 1 ist, impliziert die linke Seite von (1.5):

$$n \log(2) \leq \sum_{p \leq 2n} \left(\sum_{m=1}^{\left\lfloor \frac{\log(2n)}{\log(p)} \right\rfloor} 1 \right) \log(p) \leq \sum_{p \leq 2n} \log(2n) = \pi(2n) \log(2n).$$

Also folgt

$$(1.7) \quad \pi(2n) \geq \frac{n \log(2)}{\log(2n)} = \frac{\log(2)}{2} \frac{2n}{\log(2n)} > \frac{1}{4} \frac{2n}{\log(2n)},$$

weil $\log(2) > \frac{1}{2}$. Wegen $\frac{2n}{2n+1} \geq \frac{2}{3}$ folgt andererseits

$$\begin{aligned} \pi(2n+1) &\geq \pi(2n) > \frac{1}{4} \frac{2n}{\log(2n)} > \frac{1}{4} \cdot \frac{2n}{2n+1} \cdot \frac{2n+1}{\log(2n+1)} \\ &\geq \frac{1}{6} \frac{2n+1}{\log(2n+1)}. \end{aligned}$$

Zusammen mit (1.7) folgt, für $n \geq 2$

$$\pi(n) > \frac{1}{6} \frac{n}{\log(n)}.$$

Das beweist die erste Ungleichung. Für die zweite schätzt man die rechte Seite der Gleichung (1.6) durch den Term mit $m = 1$ ab. Da die Terme für $m > 1$ nicht-negativ sind, folgt

$$\begin{aligned} \log(2n!) - 2 \log(n!) &\geq \sum_{p \leq 2n} \left(\left[\frac{2n}{p} \right] - 2 \left[\frac{n}{p} \right] \right) \log(p) \\ &\geq \sum_{n < p \leq 2n} \log(p). \end{aligned}$$

Im letzten Schritt haben wir benutzt, daß $[2n/p] - 2[n/p] = 1$ für alle Primzahlen p im Intervall $n < p \leq 2n$ gilt. Schreiben wir $\theta(x) = \sum_{p \leq x} \log(p)$, so folgt daraus mit der rechten Seite von (1.5)

$$\theta(2n) - \theta(n) = \sum_{n < p \leq 2n} \log(p) < n \log(4).$$

Insbesondere folgt für $n = 2^r$

$$\theta(2^{r+1}) - \theta(2^r) < 2^r \log(4) = 2^{r+1} \log(2).$$

Summiert man das für $r = 0, 1, \dots, k$ auf, so steht links eine Teleskopsumme und man erhält

$$\theta(2^{k+1}) < 2^{k+2} \log(2).$$

Wenn man k so wählt, daß $2^k \leq n < 2^{k+1}$ gilt, dann folgt

$$\theta(n) \leq \theta(2^{k+1}) < 2^{k+2} \log(2) \leq 4n \log(2).$$

Das ergibt, mit $0 < \alpha < 1$,

$$(\pi(n) - \pi(n^\alpha)) \cdot \log(n^\alpha) < \sum_{n^\alpha < p \leq n} \log(p) \leq \theta(n) < 4n \log(2),$$

also

$$\begin{aligned} \pi(n) &< \frac{4n \log(2)}{\alpha \log(n)} + \pi(n^\alpha) < \frac{4n \log(2)}{\alpha \log(n)} + n^\alpha \\ &= \frac{n}{\log(n)} \left(\frac{4 \log(2)}{\alpha} + \frac{\log(n)}{n^{1-\alpha}} \right). \end{aligned}$$

Für $\alpha = \frac{2}{3}$ folgt, wenn man noch $\frac{\log(n)}{n^{1/3}} \leq \frac{3}{e}$ bedenkt,

$$\pi(n) < \frac{n}{\log(n)} \left(6 \log(2) + \frac{3}{e} \right) < 6 \frac{n}{\log(n)}.$$

Denn für $c > 0$ und $x \geq 1$ nimmt die Funktion $f(x) = x^{-c} \log(x)$ ihr Maximum bei $x = e^{1/c}$ an, d.h.,

$$\frac{\log(n)}{n^c} \leq \frac{1}{ce}.$$

□

Die Abschätzungen für $\pi(x)$ lassen sich noch verschärfen. Allerdings wächst damit der technische Aufwand für den Beweis. Außerdem gelten die Verschärfungen natürlich irgendwann nicht mehr für alle $x \geq 1$, sondern nur noch für $x \geq x_0$. Man kann zum Beispiel zeigen, daß folgende Ungleichungen gelten

$$\frac{x}{\log(x)} < \pi(x) < 1.095 \cdot \frac{x}{\log(x)}, \quad \forall x \geq 284860.$$

Die linke Ungleichung gilt schon für alle $x \geq 17$. Man beachte aber, daß noch $x/\log(x) \approx 6.0000257$ für $x = 16.999$ gilt, aber $\pi(x) = 6$. In der rechten Ungleichung kann man die Konstante verkleinern auf Kosten der Größe von x_0 , oder die Konstante vergrößern zu Gunsten von x_0 . Dazu kann man das folgende Resultat von Dusart [5] verwenden:

THEOREM 1.6.5 (Dusart). *Für reelle x gelten die folgenden Ungleichungen:*

$$\pi(x) \geq \frac{x}{\log(x)} \left(1 + \frac{1}{\log(x)} + \frac{1.8}{\log^2(x)} \right), \quad x \geq 32299,$$

$$\pi(x) \leq \frac{x}{\log(x)} \left(1 + \frac{1}{\log(x)} + \frac{2.51}{\log^2(x)} \right) < 1.094 \cdot \frac{x}{\log(x)}, \quad x \geq 355991,$$

$$\pi(x) \leq \frac{x}{\log(x)} \left(1 + \frac{1.2762}{\log(x)} \right), \quad x > 1.$$

Schon Chebyshev hatte aus solchen Abschätzungen einen Beweis für das *Bertrandsche Postulat* abgeleitet: Für jedes $n \geq 1$ enthält das Intervall $(n, 2n]$ mindestens eine Primzahl.

BEMERKUNG 1.6.6. Chebyshevs explizite Ungleichungen [4]

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

$$c_1 = \log(2^{1/2} 3^{1/3} 5^{1/5} 30^{-1/30}) \approx 0.921292022934,$$

$$c_2 = \frac{6}{5} c_1 \approx 1.10555042752$$

werden oft fälschlicherweise für $x \geq 30$ angegeben, anstatt für $x \geq 96098$, siehe [7], [8]. Die falsche Abschätzung wurde zunächst auch in einer Arbeit über die Serresche Modularitätsvermutung verwendet, siehe [11].

Weiterhin folgen aus solchen Abschätzungen auch Resultate, wie groß die n -te Primzahl p_n ist, siehe [6]:

THEOREM 1.6.7 (Dusart). *Für die n -te Primzahl p_n gelten die Abschätzungen*

$$n(\log(n) + \log(\log(n)) - 1) < p_n, \quad n \geq 1,$$

$$n(\log(n) + \log(\log(n))) > p_n, \quad n \geq 6.$$

Im Beweis von Satz 1.6.4 haben wir Chebyshevs θ -Funktion verwendet:

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

Wir wollen in diesem Zusammenhang noch zeigen:

THEOREM 1.6.8. *Der Primzahlsatz, also $\pi(x) \sim \frac{x}{\log(x)}$ für $x \rightarrow \infty$, ist äquivalent zu der Aussage $\theta(x) \sim x$ für $x \rightarrow \infty$.*

BEWEIS. Mit

$$a(n) = \begin{cases} 1 & \text{falls } n \in \mathbb{P}, \\ 0 & \text{sonst,} \end{cases}$$

hat man

$$\sum_{1 < n \leq x} a(n) = \sum_{p \leq x} 1 = \pi(x), \quad \sum_{1 < n \leq x} a(n) \log(n) = \sum_{p \leq x} \log(p) = \theta(x).$$

Nun wendet man die Abelsche Summationsformel (Satz 1.4.2) mit $f(x) = \log(x)$ und $y = 1$ an und erhält, für $x \geq 2$,

$$\theta(x) = \sum_{1 < n \leq x} a(n) \log(n) = \pi(x) \log(x) - \pi(1) \log(1) - \int_1^x \frac{\pi(t)}{t} dt.$$

Da $\pi(t) = 0$ für $t < 2$ ist, folgt

$$(1.8) \quad \theta(x) = \pi(x) \log(x) - \int_2^x \frac{\pi(t)}{t} dt.$$

Mit $b(n) = a(n) \log(n)$ hat man

$$\sum_{\frac{3}{2} < n \leq x} \frac{b(n)}{\log(n)} = \pi(x), \quad \sum_{n \leq x} b(n) = \theta(x).$$

Mit $f(x) = \frac{1}{\log(x)}$ und $y = \frac{3}{2}$ folgt aus Satz 1.4.2

$$\pi(x) = \frac{\theta(x)}{\log(x)} - \frac{\theta(\frac{3}{2})}{\log(\frac{3}{2})} + \int_{\frac{3}{2}}^x \frac{\theta(t)}{t \log^2(t)} dt.$$

Da auch $\theta(t) = 0$ ist für $t < 2$, halten wir fest:

$$(1.9) \quad \pi(x) = \frac{\theta(x)}{\log(x)} + \int_2^x \frac{\theta(t)}{t \log^2(t)} dt.$$

Wir nehmen nun an, daß $\pi(x) \sim \frac{x}{\log(x)}$ für $x \rightarrow \infty$. Dann formen wir (1.8) und (1.9) wie folgt um:

$$(1.10) \quad \frac{\theta(x)}{x} - \frac{\pi(x) \log(x)}{x} = -\frac{1}{x} \int_2^x \frac{\pi(t)}{t} dt$$

$$(1.11) \quad \frac{\pi(x) \log(x)}{x} - \frac{\theta(x)}{x} = \frac{\log(x)}{x} \int_2^x \frac{\theta(t)}{t \log^2(t)} dt.$$

Um $\theta(x) \sim x$ zu zeigen, müssen wir wegen (1.10) also nur

$$\lim_{x \rightarrow \infty} \frac{1}{x} \int_2^x \frac{\pi(t)}{t} dt = 0$$

beweisen. Nach Voraussetzung ist aber $\pi(t)/t = O(1/\log(t))$ für $t \geq 2$, also

$$\frac{1}{x} \int_2^x \frac{\pi(t)}{t} dt = O\left(\frac{1}{x} \int_2^x \frac{dt}{\log(t)}\right).$$

Es gilt aber

$$\begin{aligned} \int_2^x \frac{dt}{\log(t)} &= \int_2^{\sqrt{x}} \frac{dt}{\log(t)} + \int_{\sqrt{x}}^x \frac{dt}{\log(t)} \leq \frac{1}{\log(2)} \int_2^{\sqrt{x}} dt + \frac{1}{\log(\sqrt{x})} \int_{\sqrt{x}}^x dt \\ &\leq \frac{\sqrt{x}}{\log(2)} + \frac{x - \sqrt{x}}{\log(\sqrt{x})}. \end{aligned}$$

Das zeigt aber die Behauptung. Umgekehrt geht der Beweis analog, indem man (1.11) verwendet. Man nimmt an, daß $\lim_{x \rightarrow \infty} \theta(x)/x = 1$ ist. Um daraus den PNT zu folgern, muß man

$$\lim_{x \rightarrow \infty} \frac{\log(x)}{x} \int_2^x \frac{\theta(t) dt}{t \log^2(t)} = 0$$

zeigen. Nach Voraussetzung ist aber $\theta(t) = O(t)$, so daß

$$\frac{\log(x)}{x} \int_2^x \frac{\theta(t) dt}{t \log^2(t)} = O\left(\frac{\log(x)}{x} \int_2^x \frac{dt}{\log^2(t)}\right)$$

Wegen

$$\int_2^x \frac{dt}{\log^2(t)} \leq \frac{\sqrt{x}}{\log^2(2)} + \frac{x - \sqrt{x}}{\log^2(\sqrt{x})}$$

folgt die Behauptung. □

BEMERKUNG 1.6.9. Ebenfalls zum PNT äquivalent ist die Aussage

$$\lim_{x \rightarrow \infty} \frac{\psi(x)}{x} = 1.$$

CHAPTER 2

Periodische arithmetische Funktionen und Gauß-Summen

Viele wichtige arithmetische Funktionen sind periodisch, wie zum Beispiel Dirichlet-Charaktere. Wir wollen sie hier näher studieren.

DEFINITION 2.0.10. Sei k eine natürliche Zahl. Eine arithmetische Funktion f heißt *periodisch* mit Periode k , falls

$$f(n+k) = f(n)$$

für alle $n \in \mathbb{N}$ gilt. Die kleinste positive Periode von f heißt *Fundamentalperiode*.

Ist k eine Periode von f , dann auch mk für alle $m \in \mathbb{N}$. Zum Beispiel ist $f(n) = (n, k)$ periodisch, weil $(n+k, k) = (n, k)$ gilt. Ebenso ist die Funktion

$$f(n) = \zeta_k^n = \exp\left(\frac{2\pi in}{k}\right)$$

eine periodische arithmetische Funktion.

2.1. Dirichlet-Charaktere

Die allgemeine Definition eines Charakters auf einer Gruppe ist wie folgt:

DEFINITION 2.1.1. Ein *Charakter* f auf einer Gruppe G ist eine Abbildung $f: G \rightarrow \mathbb{C}$, die $f(ab) = f(a)f(b)$ für alle $a, b \in G$ erfüllt.

Wir verlangen, daß es ein $c \in G$ gibt mit $f(c) \neq 0$. Denn dann kann man aus $f(c)f(e) = f(c)$ nämlich $f(e) = 1$ folgern, wobei e das neutrale Element von G ist. Wenn die Gruppe G endlich ist, dann hat man $a^n = e$ für alle $a \in G$, und somit

$$f(a)^n = f(a^n) = f(e) = 1.$$

Die Werte eines Charakters auf G sind also n -te Einheitswurzeln, falls $\#G = n$. Wieviel verschiedene Charaktere hat eine endliche Gruppe G ? Man hat immer den *Hauptcharakter* auf G , der durch $f(a) = 1$ für alle $a \in G$ definiert ist. Ist die Gruppe G abelsch, so ist die Antwort wie folgt, siehe Theorem 6.8 in [1]:

THEOREM 2.1.2. *Jede endliche abelsche Gruppe G der Ordnung n hat genau n verschiedene Charaktere.*

In diesem Fall kann man auch leicht zeigen, daß die Charaktere f_i auf G selbst wieder eine Gruppe \widehat{G} bilden, unter der Multiplikation

$$(f_i f_j)(a) = f_i(a) f_j(a)$$

mit dem Einselement $f_1(a) = 1$. Die Gruppe \widehat{G} ist sogar isomorph zu G .

Sei f ein Charakter auf G . Die Funktion \overline{f} definiert durch $\overline{f}(a) = \overline{f(a)}$ ist dann ebenfalls wieder ein Charakter auf G , wegen

$$\begin{aligned} f(a)\overline{f(a)} &= |f(a)| = 1, \\ \overline{f(a)} &= \frac{1}{f(a)} = f(a^{-1}). \end{aligned}$$

Es gelten die sogenannten Orthogonalitätsrelationen, siehe Theorem 6.12 in [1]:

THEOREM 2.1.3. *Sei $G = \{a_1, \dots, a_n\}$ eine abelsche Gruppe und $\widehat{G} = \{f_1, \dots, f_n\}$. Dann gilt*

$$\sum_{\ell=1}^n \overline{f_\ell(a_i)} f_\ell(a_j) = n\delta_{ij} = \begin{cases} n & \text{falls } a_i = a_j, \\ 0 & \text{sonst.} \end{cases}$$

Ein interessanter Spezialfall tritt nun auf, wenn wir $G = (\mathbb{Z}/k\mathbb{Z})^*$ wählen. Diese Gruppe heißt auch die prime Restklassengruppe und hat $\varphi(k)$ Elemente. Die Klasse von n in dieser Gruppe sei mit \widehat{n} bezeichnet.

DEFINITION 2.1.4. Es sei f ein Charakter auf $G = (\mathbb{Z}/k\mathbb{Z})^*$. Wir definieren eine arithmetische Funktion $\chi = \chi_f$ auf ganz \mathbb{Z} durch

$$\chi(n) = \begin{cases} f(\widehat{n}) & \text{falls } (n, k) = 1, \\ 0 & \text{sonst.} \end{cases}$$

Die Funktion χ heißt *Dirichlet-Charakter modulo k* .

Der Hauptcharakter χ_1 ist also definiert durch $\chi_1(n) = 1$ für n mit $(n, k) = 1$, und $\chi_1(n) = 0$ sonst.

SATZ 2.1.5. *Ein Dirichlet-Charakter modulo k ist streng multiplikativ und periodisch mit Periode k : es gilt für alle n, m*

$$\begin{aligned} \chi(nm) &= \chi(n)\chi(m) \\ \chi(n+k) &= \chi(n). \end{aligned}$$

Es gibt $\varphi(k)$ verschiedene Dirichlet-Charaktere modulo k . Jede arithmetische Funktion χ , die diese beiden Bedingungen und $\chi(n) = 0$ für $(n, k) > 1$ erfüllt ist bereits ein Dirichlet-Charakter modulo k .

BEWEIS. Sei $G = (\mathbb{Z}/k\mathbb{Z})^*$. Da die Gruppe \widehat{G} isomorph zu G ist, gibt es $\varphi(k)$ Charaktere f für G , also $\varphi(k)$ Dirichlet-Charaktere χ_f modulo k . Für $(n, k) = (m, k) = 1$ ist

$$\chi(nm) = f(\widehat{n\widehat{m}}) = f(\widehat{n})f(\widehat{m}) = \chi(n)\chi(m).$$

Ist entweder $(n, k) > 1$ oder $(m, k) > 1$, so folgt $(nm, k) > 1$. Dann ist $\chi(nm) = 0 = \chi(n)\chi(m)$. Die Periodizität gilt, weil aus $a \equiv b(k)$ folgt $(a, k) = (b, k)$. Für die letzte Aussage bemerkt man, daß eine solche Funktion ein Charakter auf G wäre, und somit ein Dirichlet-Charakter modulo k . \square

Ist $k = 1, 2$, so gibt es wegen $\varphi(k) = 1$ nur den Hauptcharakter $\chi(1)$ mit $\chi(1) = 1$.

BEISPIEL 2.1.6. Für $k = 3$ gibt es genau zwei Dirichlet-Charaktere modulo k , nämlich

n	1	2	3
$\chi_1(n)$	1	1	0
$\chi_2(n)$	1	-1	0

In der Tat, man hat $\chi(n)^{\varphi(k)} = 1$ für $(n, k) = 1$. Für $k = 3$ bedeutet das $\chi(1)^2 = \chi(2)^2 = 1$. Es gilt $\chi(1) = 1$ und $\chi(2) = \pm 1$. Die erste Wahl des Vorzeichens führt auf χ_1 , die zweite auf χ_2 .

BEISPIEL 2.1.7. Für $k = 5$ gibt es genau vier Dirichlet-Charaktere modulo k , nämlich

n	1	2	3	4	5
$\chi_1(n)$	1	1	1	1	0
$\chi_2(n)$	1	-1	-1	1	0
$\chi_3(n)$	1	i	$-i$	-1	0
$\chi_4(n)$	1	$-i$	i	-1	0

Wegen $\varphi(5) = 4$ sind die möglichen Werte von $\chi(n)$ also gleich $1, -1, i, -i$, sofern $(n, 5) = 1$. Für $\chi(2)$ hat man also 4 Möglichkeiten. Diese legen die Tabelle fest, da $\chi(3) = \overline{\chi(2)}$ wegen $\chi(2)\chi(3) = \chi(6) = \chi(1) = 1$ und $\chi(4) = \chi(2)^2, \chi(5) = 0$.

Zur Übung fertigt man eine solche Tabelle für $k = 6$ und $k = 7$ an.

THEOREM 2.1.8. Es seien $\chi_1, \chi_2, \dots, \chi_{\varphi(k)}$ die $\varphi(k)$ verschiedenen Dirichlet-Charaktere modulo k , und $(n, k) = 1$. Dann gilt für alle $m \in \mathbb{Z}$:

$$\sum_{r=1}^{\varphi(k)} \chi_r(m) \overline{\chi_r}(n) = \begin{cases} \varphi(k) & \text{falls } n \equiv m \pmod{k}, \\ 0 & \text{sonst.} \end{cases}$$

BEWEIS. Für $(m, k) = 1$ folgt das aus Satz 2.1.3 mit $G = (\mathbb{Z}/k\mathbb{Z})^*$. Für $(m, k) > 1$ ist jeder Term in der Summe gleich Null, mit $n \not\equiv m \pmod{k}$. \square

Wir benötigen später noch Abschätzungen von Summen, in denen Dirichlet-Charaktere vorkommen.

THEOREM 2.1.9. Sei χ ein Dirichlet-Charakter modulo k mit $\chi \neq \chi_1$, weiterhin f eine nicht-negative reelle Funktion, die für alle $x \geq x_0$ eine stetige, negative Ableitung hat. Dann gilt für alle $y \geq x \geq x_0$

$$(2.1) \quad \sum_{x < n \leq y} \chi(n) f(n) = O(f(x)).$$

Falls außerdem $\lim_{x \rightarrow \infty} f(x) = 0$ gilt, so konvergiert die Reihe $\sum_{n=1}^{\infty} \chi(n) f(n)$, und für $x \geq x_0$ ist

$$(2.2) \quad \sum_{n \leq x} \chi(n)f(n) = \sum_{n=1}^{\infty} \chi(n)f(n) + O(f(x)).$$

BEWEIS. Sei $A(x) = \sum_{n \leq x} \chi(n)$. Wegen $\chi \neq \chi_1$ gibt es ein ℓ mit $(\ell, k) = 1$ und $\chi(\ell) \neq 1$. Somit ist

$$\sum_{n=1}^k \chi(n) = \sum_{n=1}^k \chi(\ell n) = \chi(\ell) \sum_{n=1}^k \chi(n),$$

und es folgt $(\chi(\ell) - 1)A(k) = 0$, also $A(k) = 0$. Wir halten das fest:

$$(2.3) \quad \sum_{n=1}^k \chi(n) = 0, \quad \chi \neq \chi_1.$$

Da χ periodisch ist, folgt $A(k) = A(2k) = A(3k) = \dots = 0$. Nun ist

$$|A(x)| = \left| \sum_{n \leq x} \chi(n) \right| < \sum_{\substack{j=1 \\ (n,k)=1}}^k 1 = \varphi(k),$$

wobei wir $|\chi(n)| \leq 1$ und $\chi(n) = 0$ für $(n, k) > 1$ verwendet haben. Also ist $A(x) = O(1)$. Das benutzen wir nun bei der Anwendung von Satz 1.4.2 (mit x und y vertauscht):

$$\begin{aligned} \sum_{x < n \leq y} \chi(n)f(n) &= A(y)f(y) - A(x)f(x) - \int_x^y A(t)f'(t)dt \\ &= O(f(y)) + O(f(x)) + O\left(\int_x^y -f'(t)dt\right) \\ &= O(f(x)). \end{aligned}$$

Das zeigt (2.1). Falls nun $f(x) \rightarrow 0$ für $x \rightarrow \infty$, so folgt daraus, daß die Reihe

$$\sum_{n=1}^{\infty} \chi(n)f(n)$$

nach dem Cauchyschen Konvergenzkriterium konvergiert. Um nun (2.2) zu zeigen, betrachte man

$$\sum_{n=1}^{\infty} \chi(n)f(n) = \sum_{n \leq x} \chi(n)f(n) + \lim_{y \rightarrow \infty} \left(\sum_{x < n \leq y} \chi(n)f(n) \right).$$

Der Limes auf der rechten Seite ist von y unabhängig. Er geht, wie gezeigt, gegen $O(f(x))$. \square

KOROLLAR 2.1.10. Sei $\chi \neq \chi_1$ ein Dirichlet-Charakter modulo k und $x \geq 1$. Dann gelten

$$(2.4) \quad \sum_{n \leq x} \frac{\chi(n)}{n} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} + O\left(\frac{1}{x}\right),$$

$$(2.5) \quad \sum_{n \leq x} \frac{\chi(n) \log(n)}{n} = \sum_{n=1}^{\infty} \frac{\chi(n) \log(n)}{n} + O\left(\frac{\log(x)}{x}\right),$$

$$(2.6) \quad \sum_{n \leq x} \frac{\chi(n)}{\sqrt{n}} = \sum_{n=1}^{\infty} \frac{\chi(n)}{\sqrt{n}} + O\left(\frac{1}{\sqrt{x}}\right).$$

BEWEIS. Man wende obigen Satz an mit $f(x) = 1/x$, beziehungsweise $f(x) = \log(x)/x$ und $f(x) = 1/\sqrt{x}$. Dann folgen die Behauptungen aus (2.2). \square

DEFINITION 2.1.11. Die L-Reihe von χ ist definiert durch

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}, \quad \operatorname{Re}(s) = \sigma > 1.$$

Diese Reihe konvergiert für $\sigma > 1$. Das obige Korollar zeigt aber, daß die folgenden Reihen auch für $s = 1$ konvergieren:

$$L(1, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-1}, \quad \chi \neq \chi_1,$$

$$L'(1, \chi) = - \sum_{n=1}^{\infty} \chi(n) \log(n) n^{-1}, \quad \chi \neq \chi_1.$$

BEMERKUNG 2.1.12. Wir werden später beweisen, daß $L(1, \chi) \neq 0$ ist für $\chi \neq \chi_1$. Das ist ein zentrales Resultat für den Beweis des Satzes von Dirichlet über Primzahlen in arithmetischen Progressionen.

2.2. Endliche Fourier-Reihen

Sei $\zeta_k = \exp\left(\frac{2\pi i}{k}\right)$ eine k -te Einheitswurzel. Dann ist, für $m \in \mathbb{Z}$, die Funktion $f(n) = \zeta_k^{nm}$ periodisch modulo k . Jede endliche Linearkombination

$$\sum_{m \in \mathbb{Z}} c(m) e^{\frac{2\pi i n m}{k}}$$

ist ebenfalls periodisch modulo k . Solche Summen heißen *endliche Fourier-Reihen*. Ein wichtiger Spezialfall sind geometrische Summen.

LEMMA 2.2.1. *Sei $k \geq 1$ fest gewählt. Dann ist*

$$\sum_{m=0}^{k-1} e^{\frac{2\pi i n m}{k}} = \begin{cases} 0 & \text{falls } k \nmid n, \\ k & \text{falls } k \mid n. \end{cases}$$

BEWEIS. Mit $x = \exp\left(\frac{2\pi i n}{k}\right)$ haben wir

$$\sum_{m=0}^{k-1} e^{\frac{2\pi i n m}{k}} = \sum_{m=0}^{k-1} x^m = \begin{cases} \frac{x^k - 1}{x - 1} & \text{falls } x \neq 1, \\ k & \text{falls } x = 1. \end{cases}$$

Wegen $x^k = 1$ ist das aber das gewünschte Resultat, denn $x = 1$ genau dann, wenn $k \mid n$. \square

Wir wollen zeigen, daß jede periodische arithmetische Funktion eine endliche Fourierentwicklung besitzt. Dazu benötigen wir

THEOREM 2.2.2 (Lagrangesches Interpolationstheorem). *Es seien z_0, z_1, \dots, z_{k-1} verschiedene komplexe Zahlen und w_0, w_1, \dots, w_{k-1} beliebige komplexe Zahlen. Dann gibt es genau ein Polynom $P(z)$ vom Grad $r \leq k - 1$, so daß $P(z_m) = w_m$ gilt für $m = 0, 1, \dots, k - 1$.*

BEWEIS. Sei $A(z) = (z - z_0)(z - z_1) \cdots (z - z_{k-1})$ und

$$A_m(z) = \frac{A(z)}{z - z_m} = (z - z_0) \cdots \widehat{(z - z_m)} \cdots (z - z_{k-1}).$$

Dann ist $A_m(z)$ ein Polynom vom Grad $k - 1$, mit $A_m(z_m) \neq 0$, aber $A_m(z_j) = 0$ für $j \neq m$. Also ist $(A_m(z_m))^{-1} A_m(z)$ ein Polynom vom Grad $k - 1$ in z , das für jedes $z = z_j$, $j \neq m$ gleich Null ist, und für $z = z_m$ gleich Eins. Nun sei

$$P(z) = \sum_{m=0}^{k-1} w_m \frac{A_m(z)}{A_m(z_m)}.$$

Es hat als Linearkombination von Polynomen des Grades $k - 1$ einen Grad $r \leq k - 1$ und erfüllt $P(z_j) = w_j$ für alle j . Dieses Polynom ist eindeutig. Wäre $Q(z)$ noch ein solches Polynom, dann hätte das Polynom $P(z) - Q(z)$ den Grad $r \leq k - 1$, aber k verschiedene Nullstellen z_0, z_1, \dots, z_{k-1} . Dann wäre $P(z) - Q(z)$ das Nullpolynom und daher $P(z) = Q(z)$. \square

Für den nächsten Satz wählen wir die z_j als k -te Einheitswurzeln.

SATZ 2.2.3. Zu gegebenen w_0, w_1, \dots, w_{k-1} aus \mathbb{C} gibt es k eindeutig bestimmte komplexe Zahlen a_0, a_1, \dots, a_{k-1} mit

$$(2.7) \quad w_m = \sum_{n=0}^{k-1} a_n e^{2\pi i n m / k}, \quad m = 0, 1, \dots, k-1.$$

Die Koeffizienten a_n sind dabei gegeben durch

$$(2.8) \quad a_n = \frac{1}{k} \sum_{m=0}^{k-1} w_m e^{-2\pi i n m / k}, \quad n = 0, 1, \dots, k-1.$$

BEWEIS. Sei $z_m = \exp(2\pi i m / k)$. Die Zahlen z_0, z_1, \dots, z_{k-1} sind dann verschieden, so daß es nach Satz 2.2.2 ein eindeutig bestimmtes Polynom

$$P(z) = \sum_{n=0}^{k-1} a_n z^n$$

gibt mit $P(z_m) = w_m$ für $m = 0, 1, \dots, k-1$. Damit sind auch die a_n eindeutig bestimmt und es folgt (2.7). Um auch (2.8) zu beweisen, multiplizieren wir (2.7) mit $\exp(-2\pi i m r / k)$, $0 \leq m, r < k$ und summieren über $m = 0$ bis $k-1$:

$$\begin{aligned} \sum_{m=0}^{k-1} w_m e^{-2\pi i m r / k} &= \sum_{n=0}^{k-1} a_n \sum_{m=0}^{k-1} e^{2\pi i (n-r)m / k} \\ &= k a_r. \end{aligned}$$

Wegen Lemma 2.2.1 ist die rechte Summe über m gleich Null für $k \nmid (n-r)$. Für $k \mid (n-r)$ hingegen folgt $n=r$ wegen $|n-r| \leq k-1$ und die Summe ist gleich k . Deshalb folgt (2.8). \square

SATZ 2.2.4. Sei f eine arithmetische Funktion, die periodisch modulo k ist. Dann gibt es eine eindeutig bestimmte arithmetische Funktion g , periodisch modulo k , mit

$$f(m) = \sum_{n=0}^{k-1} g(n) e^{2\pi i m n / k}.$$

Dabei ist g gegeben durch

$$g(n) = \frac{1}{k} \sum_{m=0}^{k-1} f(m) e^{-2\pi i m n / k}.$$

BEWEIS. Das folgt aus Satz 2.2.3 mit $w_m = f(m)$ und $g(m) = a_m$. Man erweitere g auf \mathbb{N} durch periodische Fortsetzung modulo k . \square

BEMERKUNG 2.2.5. Da f und g beide periodisch sind, können wir die Summe anstatt von 0 bis $k-1$ auch über ein beliebiges volles Restsystem modulo k laufen lassen. Wir schreiben $\sum_{n \bmod k}$

2.3. Ramanujan-Summen

Was erhält man, wenn man alle primitiven k -ten Einheitswurzeln aufsummiert ? Es kommt $\mu(k)$ heraus ! Das ist ein Spezialfall von Ramanujan-Summen.

DEFINITION 2.3.1. Seien $k, n \in \mathbb{N}$. Dann heißen die Summen

$$c_k(n) = \sum_{\substack{m \bmod k \\ (m,k)=1}} e^{2\pi i m n / k}$$

Ramanujan-Summen.

Wir benötigen noch ein Lemma:

LEMMA 2.3.2. *Es sei f eine Funktion, die auf $\mathbb{Q} \cap [0, 1]$ definiert ist und*

$$F(n) = \sum_{m=1}^n f\left(\frac{m}{n}\right), \quad G(n) = \sum_{\substack{m=1 \\ (m,n)=1}}^n f\left(\frac{m}{n}\right).$$

*Dann gilt $\mu * F = G$.*

BEWEIS. Wenn wir beachten, daß $\sum_{d|(m,n)} \mu(d) = 0$ gilt für $(m, n) > 1$, dann folgt

$$\begin{aligned} (\mu * F)(n) &= \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \left(f\left(\frac{d}{n}\right) + f\left(\frac{2d}{n}\right) + \cdots + f\left(\frac{n}{n}\right) \right) \\ &= \sum_{m=1}^n f\left(\frac{m}{n}\right) \sum_{d|(m,n)} \mu(d) = \sum_{\substack{m=1 \\ (m,n)=1}}^n f\left(\frac{m}{n}\right) = G(n). \end{aligned}$$

□

SATZ 2.3.3. *Sei $k \in \mathbb{N}$ und p eine Primzahl. Es gilt*

$$\begin{aligned} c_k(1) &= \sum_{\substack{m=1 \\ (m,k)=1}}^k (e^{2\pi i / k})^m = \mu(k), \\ c_p(1) &= \sum_{m=1}^p (e^{2\pi i / p})^m = \mu(p) = -1. \end{aligned}$$

BEWEIS. Es sei $\zeta_k = \exp\left(\frac{2\pi i}{k}\right)$ eine primitive k -te Einheitswurzel. Dann sind alle Potenzen ζ_k^m für $(m, k) = 1$ auch primitive EW (und nur diese). Wir wissen nach Lemma 2.2.1, daß die Summe *aller* k -ten EW gleich Null ist:

$$\sum_{m=1}^k \zeta_k^m = 1 + \zeta_k + \zeta_k^2 + \cdots + \zeta_k^{k-1} = 0, \quad k > 1,$$

und gleich 1 für $k = 1$. Wenn wir also $f(m/k) = \zeta_k^m$ in Lemma 2.3.2 wählen, dann folgt

$$F(k) = \sum_{m=1}^k \zeta_k^m = I(k),$$

$$G(k) = \sum_{\substack{m=1 \\ (m,k)=1}}^k \zeta_k^m = (\mu * F)(k) = (\mu * I)(k) = \mu(k).$$

□

Für $n = 1$ ist die Ramanujan-Summe also genau die μ -Funktion. Für $k \mid n$ erhalten wir die φ -Funktion zurück. Jeder Term der Summe ist dann gleich 1, und es gibt $\varphi(k)$ Terme:

$$c_k(n) = \varphi(k), \quad k \mid n.$$

Ramanujan zeigte, daß die $c_k(n)$ immer ganzzahlig sind.

DEFINITION 2.3.4. Es seien f und g zwei arithmetische Funktionen, $k, n \in \mathbb{N}$ und

$$s_k(n) = \sum_{d \mid (n,k)} f(d)g\left(\frac{k}{d}\right).$$

Die Summe ähnelt dem Dirichlet-Produkt $f * g$; allerdings summieren wir nur über gewisse Teiler d von n . Da n nur in (n, k) auftritt gilt $s_k(n+k) = s_k(n)$. Also sind die $s_k(n)$ periodische Funktionen modulo k . Somit haben sie eine endliche Fourierreihenentwicklung.

SATZ 2.3.5. Die Summen $s_k(n)$ haben die endliche Fourierreihenentwicklung

$$(2.9) \quad s_k(n) = \sum_{m \bmod k} a_k(m) e^{2\pi i m n / k}, \quad \text{mit}$$

$$(2.10) \quad a_k(m) = \sum_{d \mid (m,k)} g(d) f\left(\frac{k}{d}\right) \frac{d}{k}.$$

BEWEIS. Nach Satz 2.2.4 sind die $a_k(m)$ gegeben durch

$$\begin{aligned} a_k(m) &= \frac{1}{k} \sum_{n \bmod k} s_k(n) e^{-2\pi i n m / k} = \frac{1}{k} \sum_{n=1}^k \sum_{\substack{d|n \\ d|k}} f(d) g\left(\frac{k}{d}\right) e^{-2\pi i n m / k} \\ &= \frac{1}{k} \sum_{d|k} f(d) g\left(\frac{k}{d}\right) \sum_{c=1}^{k/d} e^{-2\pi i c d m / k} \\ &= \frac{1}{k} \sum_{d|k} f\left(\frac{k}{d}\right) g(d) \sum_{c=1}^d e^{-2\pi i c m / d}. \end{aligned}$$

Hierbei haben wir $n = cd$ geschrieben. Dann läuft der Index c , für festes d , von 1 bis k/d . Danach kann man in der Summe über c das d durch k/d ersetzen. Nach Lemma 2.2.1 ist die Summe über c gleich Null, außer für $d \mid m$, wo sie gleich d ist:

$$a_k(m) = \frac{1}{k} \sum_{\substack{d|k \\ d|m}} f\left(\frac{k}{d}\right) g(d) d = \frac{1}{k} \sum_{d|(m,k)} g(d) f\left(\frac{k}{d}\right) d.$$

□

Mit diesem Satz kann man nun die folgende Formel für $c_k(n)$ herleiten.

SATZ 2.3.6. *Es gilt*

$$c_k(n) = \sum_{d|(n,k)} \mu\left(\frac{k}{d}\right) d.$$

BEWEIS. Wir wählen $f(k) = k$ und $g(k) = \mu(k)$ in Satz 2.3.5. Dann besagt (2.9):

$$\begin{aligned} \sum_{d|(n,k)} d \mu\left(\frac{k}{d}\right) &= \sum_{m \bmod k} a_k(m) e^{2\pi i m n / k} \\ &= \sum_{m \bmod k} \sum_{d|(m,k)} \mu(d) e^{2\pi i m n / k} \\ &= \sum_{\substack{m \bmod k \\ (m,k)=1}} e^{2\pi i m n / k} = c_k(n). \end{aligned}$$

In der letzten Zeile haben wir (2.10) benutzt, was besagt

$$a_k(m) = \sum_{d|(m,k)} \mu(d) = \begin{cases} 1 & \text{falls } (m, k) = 1, \\ 0 & \text{sonst.} \end{cases}$$

□

Für $n = 1$ erhalten wir wiederum $c_k(1) = \mu(k)$ aus diesem Satz. Man sieht auch, daß die Summen $c_k(n)$ durch Spezialisierung aus den $s_k(n)$ entstehen; nämlich für $f = \text{id}$ und $g = \mu$. Wir halten noch zwei weitere Folgerungen fest, wovon die erste sofort, und die zweite für $k \mid n$ aus dem Satz folgt.

KOROLLAR 2.3.7. *Es gilt $c_k(n) \in \mathbb{Z}$ und*

$$\sum_{d|k} d\mu\left(\frac{k}{d}\right) = \varphi(k).$$

Die Summen $s_k(n)$, und damit auch die $c_k(n)$, besitzen folgende multiplikative Eigenschaften:

SATZ 2.3.8. *Es gelten folgende Identitäten:*

$$\begin{aligned} s_{mk}(ab) &= s_m(a)s_k(b), & (a, k) = (b, m) = (m, k) = 1, \\ s_m(ab) &= s_m(a), & (b, m) = 1, \\ s_{mk}(a) &= s_m(a)g(k), & (a, k) = (m, k) = 1. \end{aligned}$$

Der Beweis ist eine Übung. Die erste Identität impliziert für $k = 1$ die zweite wegen $s_1(b) = f(1)g(1) = 1$; und für $b = 1$ die dritte wegen $s_k(1) = f(1)g(k) = g(k)$. Für $c_n(k)$ gelten die Identitäten ebenso. Man muß nur $g(k) = \mu(k)$ beachten. Manchmal kann man die Summen $s_k(n)$ auch durch das Dirichlet-Produkt $f * g$ ausrechnen.

SATZ 2.3.9. *Es seien f, g, h arithmetische Funktionen mit $g(k) = \mu(k)h(k)$ und f streng multiplikativ, h multiplikativ. Es gelte $f(p) \neq 0$ und $f(p) - h(p) \neq 0$ für alle Primzahlen p . Es sei $F = f * g$. Dann folgt*

$$s_k(n) = \frac{F(k)g\left(\frac{k}{(n,k)}\right)}{F\left(\frac{k}{(n,k)}\right)}.$$

BEWEIS. Es sei $N = k/(n, k)$. Dann gilt mit Satz 1.3.12:

$$\begin{aligned} F(k) &= \sum_{d|k} f(d)\mu\left(\frac{k}{d}\right)h\left(\frac{k}{d}\right) = \sum_{d|k} f\left(\frac{k}{d}\right)\mu(d)h(d) \\ &= f(k) \sum_{d|k} \mu(d) \frac{h(d)}{f(d)} \\ &= f(k) \prod_{p|k} \left(1 - \frac{h(p)}{f(p)}\right). \end{aligned}$$

Man beachte dabei die Voraussetzungen. Insbesondere sind die Faktoren in dem Produkt nicht Null. Schreibt man $a = (n, k)$, so ist $k = aN$ und

$$\begin{aligned}
s_k(n) &= \sum_{d|a} f(d) \mu\left(\frac{k}{d}\right) h\left(\frac{k}{d}\right) = \sum_{d|a} f(d) \mu\left(\frac{aN}{d}\right) h\left(\frac{aN}{d}\right) \\
&= \sum_{d|a} f\left(\frac{a}{d}\right) \mu(Nd) h(Nd) \\
&= \mu(N) h(N) \sum_{\substack{d|a \\ (N,d)=1}} f\left(\frac{a}{d}\right) \mu(d) h(d) \\
&= f(a) \mu(N) h(N) \sum_{\substack{d|a \\ (N,d)=1}} \mu(d) \frac{h(d)}{f(d)} \\
&= f(a) \mu(N) h(N) \prod_{\substack{p|a \\ p \nmid N}} \left(1 - \frac{h(p)}{f(p)}\right) \\
&= f(a) \mu(N) h(N) \frac{\prod_{p|aN} \left(1 - \frac{h(p)}{f(p)}\right)}{\prod_{p|N} \left(1 - \frac{h(p)}{f(p)}\right)}.
\end{aligned}$$

Dabei haben wir neben Satz 1.3.12 auch noch benutzt, daß $\mu(Nd) = \mu(N)\mu(d)$ für $(N, d) = 1$ gilt, und $\mu(Nd) = 0$ sonst. Setzen wir nun die obige Formel für $F(k)$ darin ein und beachten $f(a)f(N) = f(k)$, sowie $\mu h = g$, so folgt

$$\begin{aligned}
s_k(n) &= f(a) \mu(N) h(N) \frac{F(k)}{f(k)} \frac{f(N)}{F(N)} \\
&= \frac{F(k) \mu(N) h(N)}{F(N)} = \frac{F(k) g(N)}{F(N)}.
\end{aligned}$$

□

KOROLLAR 2.3.10. *Es gilt*

$$c_k(n) = \frac{\varphi(k) \mu\left(\frac{k}{(n,k)}\right)}{\varphi\left(\frac{k}{(n,k)}\right)}.$$

BEWEIS. Man wähle $f(n) = n$ und $h(n) = 1$. Dann ist $g(n) = \mu(n)\varepsilon(n) = \mu(n)$ und $F = f * g = \text{id} * \mu = \varphi$. Für diese Spezialisierung folgt aber $s_k(n) = c_k(n)$ und die Voraussetzungen des obigen Satzes sind erfüllt. □

2.4. Gauß-Summen zu Dirichlet-Charakteren

DEFINITION 2.4.1. Es sei χ ein Dirichlet-Charakter modulo k . Dann heißt

$$G(n, \chi) = \sum_{m=1}^k \chi(m) e^{2\pi i n m / k}$$

Gauß-Summe zum Charakter χ .

Für den Hauptcharakter $\chi = \chi_1$ spezialisiert sich die Gauß-Summe zur Ramanujan-Summe, weil $\chi_1(m) = 1$ für $(m, k) = 1$ und $\chi_1(m) = 0$ sonst.

$$G(n, \chi_1) = \sum_{\substack{m=1 \\ (m,k)=1}}^k e^{2\pi i n m / k} = c_k(n).$$

SATZ 2.4.2. Für $(n, k) = 1$ gilt $G(n, \chi) = \bar{\chi}(n) G(1, \chi)$.

BEWEIS. Lläuft r durch ein vollständiges Restsystem mod k , so auch nr wegen $(n, k) = 1$. Man hat $\bar{\chi}(n)\chi(n) = |\chi(n)|^2 = 1$ und deshalb

$$\chi(r) = \bar{\chi}(n)\chi(n)\chi(r) = \bar{\chi}(n)\chi(nr).$$

Setzen wir das in $G(n, \chi)$ ein, so erhalten wir mit $m = nr$

$$\begin{aligned} G(n, \chi) &= \sum_{r \bmod k} \chi(r) e^{2\pi i n r / k} = \bar{\chi}(n) \sum_{r \bmod k} \chi(nr) e^{2\pi i n r / k} \\ &= \bar{\chi}(n) \sum_{m \bmod k} \chi(m) e^{2\pi i m / k} \\ &= \bar{\chi}(n) G(1, \chi). \end{aligned}$$

□

DEFINITION 2.4.3. Die Gauß-Summe $G(n, \chi)$ heißt *separabel*, falls gilt

$$(2.11) \quad G(n, \chi) = \bar{\chi}(n) G(1, \chi).$$

Wann ist $G(n, \chi)$ separabel, falls $(n, k) > 1$ ist ?

SATZ 2.4.4. Für natürliche Zahlen n mit $(n, k) > 1$ ist die Gauß-Summe $G(n, \chi)$ genau dann separabel, wenn $G(n, \chi) = 0$ gilt.

BEWEIS. Für $(n, k) = 1$ ist $G(n, \chi)$ separabel. Für $(n, k) > 1$ gilt $\bar{\chi}(n) = 0$, also $G(n, \chi) = 0$ nach (2.11). □

Der folgende Satz zeigt eine wichtige Konsequenz der Separabilität.

SATZ 2.4.5. Sei χ ein Dirichlet-Charakter modulo k und $G(n, \chi)$ für alle n separabel. Dann folgt

$$(2.12) \quad |G(1, \chi)|^2 = k.$$

BEWEIS. Es gilt mit (2.11)

$$\begin{aligned} |G(1, \chi)|^2 &= G(1, \chi) \overline{G(1, \chi)} = G(1, \chi) \sum_{m=1}^k \overline{\chi(m)} e^{-2\pi im/k} \\ &= \sum_{m=1}^k G(m, \chi) e^{-2\pi im/k} = \sum_{m=1}^k \sum_{r=1}^k \chi(r) e^{2\pi imr/k} e^{-2\pi im/k} \\ &= \sum_{r=1}^k \chi(r) \sum_{m=1}^k e^{2\pi im(r-1)/k} = k\chi(1) = k. \end{aligned}$$

Dabei haben wir Lemma 2.2.1 verwendet: die letzte Summe von $m = 1$ bis k ist gleich k , falls $r = 1$ ist, und Null sonst. Man hat $k \nmid (r-1)$, außer für $r = 1$. \square

Falls $(n, k) > 1$ gilt, möchte man wissen, wann $G(n, \chi)$ gleich Null bzw. ungleich Null ist.

SATZ 2.4.6. Es gelte $G(n, \chi) \neq 0$ für ein n mit $(n, k) > 1$. Dann gibt es einen Teiler $d \mid k$, $d < k$, so daß für alle a mit $(a, k) = 1$ und $a \equiv 1(d)$ gilt $\chi(a) = 1$.

BEWEIS. Es sei $q = (n, k)$ und $d = k/q$. Dann gilt $d \mid k$ und $d \neq k$ wegen $q \neq 1$. Man wähle irgendein a mit $(a, k) = 1$ und $a \equiv 1(d)$. Wir wollen $\chi(a) = 1$ zeigen. Wegen $(a, k) = 1$ dürfen wir in der Summe, die $G(n, \chi)$ definiert, den Index m durch am ersetzen, d.h.,

$$\begin{aligned} G(n, \chi) &= \sum_{m \bmod k} \chi(m) e^{2\pi inm/k} = \sum_{m \bmod k} \chi(am) e^{2\pi ianm/k} \\ &= \chi(a) \sum_{m \bmod k} \chi(m) e^{2\pi ianm/k}. \end{aligned}$$

Wegen $a \equiv 1(d)$ und $d = k/q$ können wir $a = 1 + bk/q$ mit $b \in \mathbb{Z}$ schreiben. Dann ist wegen $q \mid n$

$$\frac{anm}{k} = \frac{nm}{k} + \frac{bknm}{qk} = \frac{nm}{k} + c$$

für ein $c \in \mathbb{Z}$. Daraus folgt $e^{2\pi ianm/k} = e^{2\pi inm/k}$ und somit

$$G(n, \chi) = \chi(a) \sum_{m \bmod k} \chi(m) e^{2\pi inm/k} = \chi(a) G(n, \chi).$$

Wegen $G(n, \chi) \neq 0$ folgt $\chi(a) = 1$. \square

Der obige Satz legt es nahe, Dirichlet-Charaktere χ mit einer solchen Eigenschaft auszuzeichnen.

DEFINITION 2.4.7. Sei χ ein Dirichlet-Charakter modulo k . Ein positiver Teiler $d \mid k$ heißt *induzierte Restklassenordnung* für χ , falls $\chi(a) = 1$ für alle a mit $(a, k) = 1$ und $a \equiv 1(d)$ gilt.

Man beachte, daß $d = k$ selbst auch eine induzierte Restklassenordnung für χ ist. Wann ist $d = 1$ eine induzierte Restklassenordnung für χ ?

SATZ 2.4.8. Für einen Dirichlet-Charakter χ modulo k ist $d = 1$ genau dann eine induzierte Restklassenordnung für χ , falls $\chi = \chi_1$ ist.

BEWEIS. Wenn $\chi = \chi_1$ ist, dann gilt $\chi(a) = 1$ überhaupt für alle a mit $(a, k) = 1$. Die Bedingung $a \equiv 1(1)$ gilt für alle a . Also ist $d = 1$ eine induzierte Restklassenordnung für χ_1 . Ist umgekehrt $d = 1$ eine induzierte Restklassenordnung, so gilt $\chi(a) = 1$ für alle a mit $(a, k) = 1$, und $\chi(a) = 0$ für $(a, k) > 1$. Das bedeutet $\chi = \chi_1$. \square

Dirichlet-Charaktere, die nur $d = k$ als induzierte Restklassenordnung besitzen, bekommen einen besonderen Namen.

DEFINITION 2.4.9. Ein Dirichlet-Charakter modulo k heißt *primitiv mod k* , falls er keine induzierte Restklassenordnung $d < k$ besitzt.

Also ist χ primitiv mod k , falls es für jeden Teiler $d \mid k$, $0 < d < k$ ein $a \in \mathbb{N}$ gibt mit $a \equiv 1(d)$ und $(a, k) = 1$, so daß gilt $\chi(a) \neq 1$.

SATZ 2.4.10. Sei χ ein Dirichlet-Charakter modulo p , wobei p prim ist und $\chi \neq \chi_1$. Dann ist χ primitiv mod p .

BEWEIS. Für induzierte Restklassenordnungen kommen nur Teiler von p in Frage, also $d = 1$ oder $d = p$. Wegen $\chi \neq \chi_1$ und Satz 2.4.8 ist $d = 1$ aber keine induzierte Restklassenordnung. Also hat χ keine induzierte Restklassenordnung $d < p$. \square

Die Sätze 2.4.4, 2.4.5, 2.4.6 kann man nun folgendermaßen formulieren.

THEOREM 2.4.11. Sei χ ein primitiver Dirichlet-Charakter modulo k . Dann gelten:

- (a) $G(n, \chi) = 0$ für alle n mit $(n, k) > 1$.
- (b) $G(n, \chi)$ ist für alle n separabel.
- (c) $|G(1, \chi)|^2 = k$.

BEWEIS. Gäbe es ein n mit $(n, k) > 1$ und $G(n, \chi) \neq 0$, so wäre χ nach Satz 2.4.6 nicht primitiv. Widerspruch. Also folgt (a).

Für $(n, k) = 1$ ist $G(n, \chi)$ separabel. Wegen Satz 2.4.4 und Teil (a) ist $G(n, \chi)$ auch separabel für $(n, k) > 1$. Also folgt (b).

Teil (c) folgt aus (b) und Satz 2.4.5. \square

SATZ 2.4.12. Sei d ein positiver Teiler von k und χ ein Dirichlet-Charakter modulo k . Dann ist d eine induzierte Restklassenordnung für χ genau dann, wenn

$$(2.13) \quad \chi(a) = \chi(b) \quad \forall a, b \text{ mit } (a, k) = (b, k) = 1, a \equiv b(d).$$

BEWEIS. Aus (2.13) folgt für die Wahl $b = 1$, daß d eine induzierte Restklassenordnung für χ ist. Sei also umgekehrt d eine induzierte Restklassenordnung. Seien a, b mit $(a, k) = (b, k) = 1$ und $a \equiv b(d)$ vorgelegt. Wegen $(a, k) = 1$ existiert ein a' mit $aa' \equiv 1(k)$, also auch mit $aa' \equiv 1(d)$ wegen $d \mid k$. Nach Voraussetzung folgt $\chi(aa') = 1$. Wegen $a \equiv b(d)$ hat man auch

$aa' \equiv ba' \equiv 1(d)$ und somit

$$1 = \chi(aa') = \chi(ba') = \chi(a)\chi(a') = \chi(b)\chi(a').$$

Diese Gleichung besagt auch $\chi(a') \neq 0$, also folgt $\chi(a')^{-1} = \chi(a) = \chi(b)$. \square

BEISPIEL 2.4.13. Die folgende Tabelle beschreibt einen Charakter modulo 9, für den $d = 3$ eine induzierte Restklassenordnung ist:

n	1	2	3	4	5	6	7	8	9
$\chi(n)$	1	-1	0	1	-1	0	1	-1	0

Offensichtlich ist (2.13) mit $d = 3$ erfüllt. χ ist periodisch modulo 3. Der Charakter ist eine Erweiterung des Charakters ψ mit $\psi(1) = 1, \psi(2) = -1$ und $\psi(3) = 0$, welcher nach Satz 2.4.10 primitiv ist.

BEISPIEL 2.4.14. Sei χ der folgende Dirichlet-Charakter modulo 6:

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

Nur 1 und 5 sind teulfremd zu 6. Davon ist nur $n = 1$ kongruent 1 mod 3. Also ist klar, daß $d = 3$ eine induzierte Restklassenordnung für χ ist. Allerdings ist χ hier keine Erweiterung irgendeines Charakters modulo 3, von denen ja keiner $\chi(2) = 0$ erfüllt.

SATZ 2.4.15. Es sei χ ein Dirichlet-Charakter modulo k und $d \mid k, d > 0$. Dann sind folgende Aussagen äquivalent:

- (a) d ist eine induzierte Restklassenordnung für χ .
- (b) Es gibt einen Charakter ψ modulo d mit $\chi(n) = \psi(n)\chi_1(n)$.

BEWEIS. Es gelte (b). Wähle ein n mit $(n, k) = 1$ und $n \equiv 1(d)$. Dann ist $\chi_1(n) = \psi(n) = 1$ nach Definition. Also ist $\chi(n) = 1$ für solche n und d eine induzierte Restklassenordnung. Es gelte (a). Wir müssen ein passendes ψ konstruieren. Für $(n, d) > 1$ setzen wir $\psi(n) = 0$. Dann ist auch $(n, k) > 1$ und $\chi(n) = 0 = \psi(n)\chi_1(n)$. Sei nun $(n, d) = 1$. Wir behaupten

$$(2.14) \quad \text{Es gibt ein } m \in \mathbb{Z} \text{ mit } m \equiv n(d), (m, k) = 1.$$

Man kann (2.14) elementar beweisen (Übung). Es folgt natürlich aus Dirichlets Theorem, weil die Folge der Zahlen $xd + n, x \in \mathbb{N}$ unendlich viele Primzahlen enthält und deshalb auch eine Primzahl m die $m \nmid k$ erfüllt. Wie auch immer, man fixiere ein solches m , welches eindeutig modulo d ist und definiere $\psi(n) = \chi(m)$. Das ist wohldefiniert, weil $\chi(a) = \chi(b)$ für $a \equiv b(d)$ und $(a, k) = (b, k) = 1$. Damit ist ψ ein Charakter modulo d . Es bleibt die angegebene Eigenschaft für $(n, k) = 1$, also $(n, d) = 1$ zu zeigen. Es ist $\psi(n) = \chi(m)$ für $m \equiv n(d)$. Wegen (a), $\chi_1(n) = 1$ und Satz 2.4.7 gilt

$$\chi(n) = \chi(m) = \psi(n) = \psi(n)\chi_1(n).$$

\square

DEFINITION 2.4.16. Sei χ ein Dirichlet-Charakter modulo k . Die kleinste induzierte Restklassenordnung d für χ heißt *Führer* von χ .

SATZ 2.4.17. Jeder Dirichlet-Charakter χ modulo k kann als Produkt $\chi(n) = \psi(n)\chi_1(n)$ geschrieben werden, wobei ψ ein primitiver Charakter modulo d ist, und d der Führer von χ .

BEWEIS. Wegen Satz 2.4.15 läßt sich χ so schreiben. Wir müssen nur zeigen, daß ψ primitiv ist. Angenommen, das ist nicht der Fall. Dann gibt es einen Teiler $q \mid d$ mit $q < d$, also auch $q \mid k$, der eine induzierte Restklassenordnung für ψ ist. Für n mit $n \equiv 1(q)$ und $(n, k) = 1$ gilt

$$1 = \psi(1) = \psi(n) = \psi(n)\chi_1(n) = \chi(n),$$

weil q eine induzierte Restklassenordnung für ψ ist. Damit ist q aber auch eine Restklassenordnung für χ . Das ist ein Widerspruch, da d der Führer von χ ist, also die kleinste induzierte Restklassenordnung. \square

Wir wenden uns nun wieder den Gauß-Summen zu:

THEOREM 2.4.18. Sei χ ein Dirichlet-Charakter modulo k . Dann ist χ genau dann primitiv modulo k , wenn die Gauß-Summe $G(n, \chi)$ für alle n separabel ist.

BEWEIS. Wenn χ primitiv ist, dann ist $G(n, \chi)$ wegen Theorem 2.4.11 separabel für alle n . Umgekehrt genügt es nach Satz 2.4.2 und 2.4.4 zu zeigen: ist χ nicht primitiv, dann gilt $G(r, \chi) \neq 0$ für ein r mit $(r, k) > 1$ (für $(r, k) = 1$ ist $G(r, \chi)$ immer separabel, für $(r, k) > 1$ genau dann, wenn $G(r, \chi) = 0$ gilt). Sei also χ nicht primitiv modulo k , also $k > 1$. Es bezeichne $d < k$ den Führer von χ mit $r = k/d$. Es ist $(r, k) > 1$ weil $d \mid k$ gilt. Wegen Satz 2.4.17 gibt es einen primitiven Charakter ψ modulo d mit $\chi(n) = \psi(n)\chi_1(n)$. Also ist

$$\begin{aligned} G(r, \chi) &= \sum_{m \bmod k} \psi(m)\chi_1(m)e^{2\pi irm/k} = \sum_{\substack{m \bmod k \\ (m, k)=1}} \psi(m)e^{2\pi irm/k} \\ &= \sum_{\substack{m \bmod k \\ (m, k)=1}} \psi(m)e^{2\pi im/d} \\ &= \frac{\varphi(k)}{\varphi(d)} \sum_{\substack{m \bmod d \\ (m, d)=1}} \psi(m)e^{2\pi im/d} \\ &= \frac{\varphi(k)}{\varphi(d)} G(1, \psi). \end{aligned}$$

Wegen Theorem 2.4.11 gilt $|G(1, \psi)|^2 = d$, weil ψ primitiv ist. Das bedeutet aber $G(r, \chi) \neq 0$, was wir zeigen wollten. Für die vorletzte Gleichung oben haben wir folgende Tatsache verwendet, siehe [1] Theorem 5.33:

Sei S ein reduziertes Restsystem modulo k und $d \mid k$ ein positiver Teiler (ein solches S ist eine Menge von $\varphi(k)$ zu k teilerfremden Zahlen, die paarweise inkongruent modulo k sind). Dann ist S die Vereinigung von $\varphi(k)/\varphi(d)$ disjunkten Mengen, die alle reduzierte Restsysteme modulo d sind. \square

2.5. Pólyas Ungleichung für Dirichlet-Charaktere

Da jeder Dirichlet-Charakter χ modulo k auch periodisch modulo k ist, hat er eine endliche Fourierentwicklung

$$(2.15) \quad \chi(m) = \sum_{n=1}^k a_k(n) e^{2\pi i m n / k}$$

wobei die Koeffizienten nach Satz 2.2.4 gegeben sind durch

$$(2.16) \quad a_k(n) = \frac{1}{k} \sum_{m=1}^k \chi(m) e^{-2\pi i m n / k} = \frac{1}{k} G(-n, \chi).$$

Ist χ nun primitiv, so kann die Fourierentwicklung (2.15) wie folgt dargestellt werden.

SATZ 2.5.1. *Die endliche Fourierentwicklung eines primitiven Dirichlet-Charakters χ modulo k hat die Form*

$$(2.17) \quad \chi(n) = \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{m=1}^k \bar{\chi}(m) e^{-2\pi i m n / k}, \quad \text{wobei}$$

$$(2.18) \quad \tau_k(\chi) = \frac{G(1, \chi)}{\sqrt{k}}, \quad |\tau_k(\chi)| = 1.$$

BEWEIS. Da χ primitiv ist, muß $G(-n, \chi)$ separabel sein nach Theorem 2.4.18. Also ist $G(-n, \chi) = \bar{\chi}(-n)G(1, \chi)$ und (2.16) impliziert $a_k(n) = \frac{1}{k} \bar{\chi}(-n)G(1, \chi)$. Damit schreibt sich (2.15) wie folgt (mit n und m vertauscht)

$$\begin{aligned} \chi(n) &= \frac{G(1, \chi)}{k} \sum_{m=1}^k \bar{\chi}(-m) e^{2\pi i m n / k} \\ &= \frac{G(1, \chi)}{k} \sum_{m=1}^k \bar{\chi}(m) e^{-2\pi i m n / k}. \end{aligned}$$

Doch das ist gleichwertig mit (2.17), und $\tau_k(\chi)$ ist so normiert, daß

$$|\tau_k(\chi)| = \frac{|G(1, \chi)|}{\sqrt{k}} = \frac{\sqrt{k}}{\sqrt{k}} = 1.$$

□

Nun kommen wir zu Pólyas Ungleichung. Für χ modulo k und $x \geq 1$ sei

$$A_\chi(x) = \sum_{n \leq x} \chi(n).$$

Wir hatten in Theorem 2.1.9 schon gezeigt, daß $|A_\chi(x)| < \varphi(k)$ gilt für $\chi \neq \chi_1$. Für $\chi = \chi_1$ ist schon $A_{\chi_1}(k) = \varphi(k)$, also eine solche Ungleichung unmöglich. Man kann die Ungleichung aber für primitive Charaktere noch verbessern.

THEOREM 2.5.2 (Pólya). *Sei χ ein primitiver Dirichlet-Charakter modulo k und $x \geq 1$. Dann gilt*

$$|A_\chi(x)| < \sqrt{k} \log(k).$$

BEWEIS. Wir schreiben $\chi(n)$ so wie in (2.17) und summieren über alle $n \leq x$. Dann folgt, mit $\chi(k) = 0$,

$$\begin{aligned} \sum_{n \leq x} \chi(n) &= \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{m=1}^{k-1} \bar{\chi}(m) \sum_{n \leq x} e^{-2\pi i n m / k} \\ &= \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{m=1}^{k-1} \bar{\chi}(m) f(m), \end{aligned}$$

wobei wir die letzte Summe mit $f(m)$ abgekürzt haben. Multiplizieren wir diese Gleichung mit \sqrt{k} und nehmen Absolutbeträge, so folgt wegen $|\tau_k(\chi)| = 1$

$$(2.19) \quad \sqrt{k} \cdot \left| \sum_{n \leq x} \chi(n) \right| \leq \sum_{m=1}^{k-1} |f(m)|.$$

Wegen $f(k-m) = \overline{f(m)}$ gilt $|f(k-m)| = |f(m)|$. Deshalb folgt aus (2.19)

$$(2.20) \quad \sqrt{k} \cdot |A_\chi(x)| \leq \begin{cases} 2 \sum_{m < k/2} |f(m)| & \text{falls } k \equiv 1(2), \\ 2 \sum_{m < k/2} |f(m)| + |f(k/2)| & \text{falls } k \equiv 0(2). \end{cases}$$

Nun ist $f(m)$ eine geometrische Summe der Form $f(m) = \sum_{n=1}^r y^n$ mit $r = [x]$, $y = e^{-2\pi i m / k}$. Wegen $1 \leq m \leq k-1$ ist $y \neq 1$. Mit $z = e^{-\pi i m / k}$ haben wir $y = z^2$ und $z^2 \neq 1$. Also folgt

$$f(m) = y \cdot \frac{y^r - 1}{y - 1} = z^2 \cdot \frac{z^{2r} - 1}{z^2 - 1} = z^{r+1} \cdot \frac{z^r - z^{-r}}{z - z^{-1}}.$$

Wegen $|z| = 1$ folgt

$$|f(m)| = \left| \frac{z^r - z^{-r}}{z - z^{-1}} \right| = \frac{|\sin(\frac{\pi r m}{k})|}{|\sin(\frac{\pi m}{k})|} \leq \frac{1}{\sin(\frac{\pi m}{k})}.$$

Da $\sin(t) \geq 2t/\pi$ gilt für $0 \leq t \leq \pi/2$, folgt mit $t = \pi m/k$

$$|f(m)| \leq \frac{1}{\frac{2}{\pi} \frac{\pi m}{k}} = \frac{k}{2m}.$$

Nun untersuchen wir damit (2.20) für gerade und ungerade k . Für $k \equiv 1(2)$ folgt

$$\sqrt{k} \cdot |A_\chi(x)| \leq k \cdot \sum_{m < k/2} \frac{1}{m} < k \log(k),$$

und für $k \equiv 0(2)$ folgt

$$\sqrt{k} \cdot |A_\chi(x)| \leq k \cdot \left(\sum_{m < k/2} \frac{1}{m} + \frac{1}{k} \right) < k \log(k).$$

□

BEMERKUNG 2.5.3. Man kann sogar auch $|A_\chi(x)| < \sqrt{k} + \frac{2}{\pi} \sqrt{k} \log(k)$ zeigen, also den Hauptterm noch um den Faktor $2/\pi$ verbessern.

2.6. Quadratische Gauß-Summen

Wir beginnen mit der Definition quadratischer (Nicht)-Reste.

DEFINITION 2.6.1. Sei $p \in \mathbb{P}$ und $n \in \mathbb{N}$ mit $p \nmid n$. Falls die Kongruenz $x^2 \equiv n \pmod{p}$ lösbar ist, so heißt n ein *quadratischer Rest modulo p* . Andernfalls heißt n ein *quadratischer Nichtrest modulo p* .

BEISPIEL 2.6.2. Es sind $\{1, 3, 4, 5, 9\}$ die quadratischen Reste modulo 11 und $\{2, 6, 7, 8, 10\}$ die quadratischen Nichtreste modulo 11.

Nehmen wir ein Restsystem modulo 11, zum Beispiel $\{0, 1, \dots, 10\}$, und berechnen ihre Quadrate modulo 11. Dann bekommen wir genau diese Reste ($1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 9, 4^2 \equiv 5$ etc.). Wegen $11 \nmid n$ ist $n = 0$ nicht zugelassen. Es ist kein Zufall, daß beide Mengen gleich viele Elemente haben.

SATZ 2.6.3. Sei $p > 2$ eine Primzahl. Dann enthält jedes reduzierte Restsystem modulo p genau $(p-1)/2$ quadratische Reste, und genau $(p-1)/2$ quadratische Nichtreste.

BEWEIS. Es sei $S = \{1^2, 2^2, \dots, (\frac{p-1}{2})^2\}$. Die Zahlen sind alle inkongruent modulo p : falls $x^2 \equiv y^2 \pmod{p}$ gilt mit $1 \leq x, y \leq (p-1)/2$, so folgt $(x-y)(x+y) \equiv 0 \pmod{p}$. Da aber $1 < x+y < p$ gilt, ist $x-y \equiv 0 \pmod{p}$ und deshalb $x=y$. Jeder quadratische Rest modulo p ist zu genau einer der Zahlen aus S kongruent wegen $(p-k)^2 \equiv k^2 \pmod{p}$. Die Menge S hat $\frac{p-1}{2}$ Elemente. \square

DEFINITION 2.6.4. Es sei $p > 2$ eine Primzahl und $n \in \mathbb{Z}$. Das *Legendre-Symbol* ist definiert als

$$\left(\frac{n}{p}\right) = \begin{cases} +1 & \text{falls } n \text{ quadratischer Rest modulo } p \text{ ist,} \\ -1 & \text{falls } n \text{ quadratischer Nichtrest modulo } p \text{ ist,} \\ 0 & \text{falls } n \equiv 0 \pmod{p} \text{ ist.} \end{cases}$$

THEOREM 2.6.5 (Euler). Sei $p > 2$ eine Primzahl, Dann gilt für alle n

$$\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \pmod{p}.$$

Einen Beweis findet man zum Beispiel in [1], Theorem 9.2.

KOROLLAR 2.6.6. Das Legendre-Symbol $\chi(n) = (n | p)$ ist eine streng multiplikative Funktion.

BEWEIS. Für $p \mid m$ oder $p \mid n$ folgt $p \mid nm$, so daß beide Seiten gleich Null sind. Für $p \nmid n, p \nmid m$ hat man

$$\left(\frac{nm}{p}\right) \equiv (nm)^{(p-1)/2} = n^{(p-1)/2} m^{(p-1)/2} \equiv \left(\frac{n}{p}\right) \left(\frac{m}{p}\right) \pmod{p}.$$

Die linke und die rechte Seite kann nur die Werte 1 oder -1 annehmen. Die Differenz

$$\left(\frac{nm}{p}\right) - \left(\frac{n}{p}\right)\left(\frac{m}{p}\right)$$

ist also gleich 0, 2 oder -2 . Da sie aber durch $p > 2$ teilbar ist, ist sie gleich Null. \square

BEMERKUNG 2.6.7. Da das Legendre-Symbol streng multiplikativ ist, periodisch modulo p und bei $p \mid n$ verschwindet, ist es ein Dirichlet-Charakter χ modulo p , der $\chi^2 = \chi_1$ erfüllt. Ein solcher Charakter heißt *quadratisch*.

Gauß hat 1796 das folgende berühmte quadratische Reziprozitätsgesetz bewiesen.

THEOREM 2.6.8. *Für ungerade, verschiedene Primzahlen p und q gilt*

$$\begin{aligned} \left(\frac{-1}{p}\right) &= (-1)^{(p-1)/2}, \\ \left(\frac{2}{p}\right) &= (-1)^{(p^2-1)/8}, \\ \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \end{aligned}$$

Damit ist $(-1 \mid p) = 1$, falls $p \equiv 1(4)$, und $(2 \mid p) = 1$, falls $p \equiv \pm 1(8)$. Der dritte Teil besagt, daß $(p \mid q) = (q \mid p)$ gilt, es sei denn man hat $p \equiv q \equiv 3(4)$, wo $(p \mid q) = -(q \mid p)$ gilt. Damit kann man rekursiv entscheiden, ob ein p quadratischer Rest modulo q ist, oder nicht.

BEISPIEL 2.6.9. $p = 1997$ ist ein quadratischer Nichtrest modulo $q = 1999$.

Man beachte, daß 1997 und 1999 Primzahlzwillinge sind. Als solche sind sie nie gleichzeitig kongruent 3 modulo 4. Also ist $(1997 \mid 1999) = (1999 \mid 1997) = (2 \mid 1997)$. Sind $p, p+2$ Primzahlen, so folgt allgemein

$$\left(\frac{p}{p+2}\right) = \left(\frac{p+2}{p}\right) = \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

In unserem Fall ist $(2 \mid 1997) = -1$, da $1997 \equiv -3 \pmod{8}$ ist. Es gibt viele Beweise für das Reziprozitätsgesetz. Einige davon benutzen *quadratische Gauß-Summen*

$$G(n, \chi) = \sum_{r \bmod p} \chi(r) e^{2\pi i nr/p}, \quad \chi(r) = \left(\frac{r}{p}\right).$$

Da p eine Primzahl ist, ist der quadratische Charakter $\chi(r) = (r \mid p)$ primitiv. Also ist die Gauß-Summe separabel, d.h., $G(n, \chi) = (n \mid p)G(1, \chi)$.

DEFINITION 2.6.10. Es sei χ der Legendre-Charakter modulo p . Dann bezeichnen wir mit $g(\chi)$ die quadratische Gauß-Summe

$$g(\chi) = G(1, \chi) = \sum_{r=1}^p \left(\frac{r}{p}\right) e^{2\pi ir/p}.$$

Wir wissen schon, daß $|g(\chi)| = \sqrt{p}$ für $p > 2$ gilt. Nun beweisen wir $g(\chi)^2 = \pm p$.

SATZ 2.6.11. Sei χ der Legendre-Charakter modulo p . Dann gilt

$$g(\chi)^2 = \left(\frac{-1}{p}\right) p = (-1)^{(p-1)/2} p.$$

BEWEIS. Es gilt

$$g(\chi)^2 = \sum_{r=1}^{p-1} \sum_{s=1}^{p-1} \left(\frac{r}{p}\right) \left(\frac{s}{p}\right) e^{2\pi i(r+s)/p}.$$

Das schreiben wir um. Für jedes Paar r, s gibt es ein eindeutiges $t \bmod p$ mit $s \equiv tr(p)$. Also ist

$$\left(\frac{r}{p}\right) \left(\frac{s}{p}\right) = \left(\frac{r}{p}\right) \left(\frac{tr}{p}\right) = \left(\frac{r^2}{p}\right) \left(\frac{t}{p}\right) = \left(\frac{t}{p}\right),$$

also folgt

$$\begin{aligned} g(\chi)^2 &= \sum_{t=1}^{p-1} \sum_{r=1}^{p-1} \left(\frac{t}{p}\right) e^{2\pi i r(1+t)/p} \\ &= \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) \sum_{r=1}^{p-1} e^{2\pi i r(1+t)/p} \\ &= - \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) + p \left(\frac{p-1}{p}\right) \\ &= \left(\frac{-1}{p}\right) p. \end{aligned}$$

Dabei haben wir benutzt, daß die Summe von $r = 1$ bis $p - 1$ gleich -1 ist, falls $p \nmid (1+t)$, und p andernfalls. Das Legendre-Symbol $(t | p)$ ist genau $\frac{p-1}{2}$ -mal $+1$ und $\frac{p-1}{2}$ -mal -1 , so daß man $\sum_{t=1}^{p-1} \left(\frac{t}{p}\right) = 0$ hat. \square

Nun wissen wir, daß $g(\chi)$ den Wert $\pm\sqrt{p}$ hat, falls $p \equiv 1(4)$, und $\pm i\sqrt{p}$, falls $p \equiv 3(4)$. Das richtige Vorzeichen zu finden ist nicht leicht. Gauß trug 1801 in sein Tagebuch ein, daß er glaube, es gälte immer das Pluszeichen, unabhängig von der Wahl von p . Er brauchte 4 Jahre, um das wirklich zu beweisen. Am dritten September 1805 schrieb er: *Wie der Blitz einschlägt, hat sich das Rätsel gelöst!*

THEOREM 2.6.12 (Gauß). Sei $\chi(r) = \left(\frac{r}{p}\right)$. Dann gilt

$$g(\chi) = \begin{cases} \sqrt{p} & \text{falls } p \equiv 1(4), \\ i\sqrt{p} & \text{falls } p \equiv 3(4). \end{cases}$$

BEWEIS. Sei $\zeta = e^{2\pi i/p}$ eine p -te EW. Dann sind $1, \zeta, \zeta^2, \dots, \zeta^{p-1}$ die Wurzeln des Polynoms $x^p - 1$ über \mathbb{C} . Wir zeigen zuerst folgende Identität:

$$(2.21) \quad \prod_{k=1}^{(p-1)/2} (\zeta^{2k-1} - \zeta^{-(2k-1)})^2 = (-1)^{(p-1)/2} p.$$

Wir haben nämlich

$$\begin{aligned} x^p - 1 &= (x - 1) \prod_{j=1}^{p-1} (x - \zeta^j), \\ \frac{x^p - 1}{x - 1} &= 1 + x + x^2 + \dots + x^{p-1} = \prod_{j=1}^{p-1} (x - \zeta^j). \end{aligned}$$

In der letzten Gleichung dürfen wir $x = 1$ setzen und erhalten

$$p = \prod_{\substack{r \bmod p \\ r \neq 0}} (1 - \zeta^r),$$

wobei das Produkt über jedes vollständige Restsystem modulo p ohne Null laufen kann. Wählt man zum Beispiel die Zahlen $\pm(4k - 2)$ für $k = 1, 2, \dots, \frac{p-1}{2}$, so folgt

$$\begin{aligned} p &= \prod_{k=1}^{(p-1)/2} (1 - \zeta^{4k-2}) \prod_{k=1}^{(p-1)/2} (1 - \zeta^{-(4k-2)}) \\ &= \prod_{k=1}^{(p-1)/2} (\zeta^{-(2k-1)} - \zeta^{2k-1}) \prod_{k=1}^{(p-1)/2} (\zeta^{2k-1} - \zeta^{-(2k-1)}) \\ &= (-1)^{(p-1)/2} \prod_{k=1}^{(p-1)/2} (\zeta^{2k-1} - \zeta^{-(2k-1)})^2. \end{aligned}$$

Damit ist (2.21) gezeigt. Wir ziehen nun die Wurzel daraus, deren Vorzeichen wir leicht bestimmen können:

$$(2.22) \quad \prod_{k=1}^{(p-1)/2} (\zeta^{2k-1} - \zeta^{-(2k-1)}) = \begin{cases} \sqrt{p} & \text{falls } p \equiv 1(4), \\ i\sqrt{p} & \text{falls } p \equiv 3(4). \end{cases}$$

Wir zeigen, daß hier jeder Faktor links von der Form α oder $i\alpha$ ist, mit $\alpha > 0$. Also ist die positive Wurzel auf der rechten Seite korrekt. Man hat

$$\begin{aligned} \prod_{k=1}^{(p-1)/2} (\zeta^{2k-1} - \zeta^{-(2k-1)}) &= \prod_{k=1}^{(p-1)/2} 2i \left(\frac{1}{2i} (e^{2\pi i/p})^{2k-1} - \frac{1}{2i} (e^{-2\pi i/p})^{2k-1} \right) \\ &= (i)^{(p-1)/2} \prod_{k=1}^{(p-1)/2} 2 \sin \left(\frac{(4k-2)\pi}{p} \right). \end{aligned}$$

Hier gilt $\sin((4k-2)\pi/p) < 0$ für $(p+2)/4 < k \leq (p-1)/2$. Das Sinusprodukt hat also genau

$$\frac{p-1}{2} - \left\lfloor \frac{p+2}{4} \right\rfloor = \begin{cases} \frac{p-1}{4} & \text{falls } p \equiv 1(4), \\ \frac{p-3}{4} & \text{falls } p \equiv 3(4) \end{cases}$$

negative Terme, also den Faktor $(-1)^{(p-1)/4}$ oder $(-1)^{(p-3)/4}$. Andererseits ist

$$i^{(p-1)/2} = \begin{cases} (-1)^{(p-1)/4} & \text{falls } p \equiv 1(4), \\ i(-1)^{(p-3)/4} & \text{falls } p \equiv 3(4). \end{cases}$$

Zusammen erhält man für beide Fälle von p modulo 4 eine *gerade* Potenz von -1 für das Produkt in (2.22), also jeweils das positive Vorzeichen.

Mit (2.21), (2.22) und Satz 2.6.11 weiß man also

$$\begin{aligned} g(\chi)^2 &= (-1)^{(p-1)/2} p = \prod_{k=1}^{(p-1)/2} (\zeta^{2k-1} - \zeta^{-(2k-1)})^2, \\ g(\chi) &= \varepsilon \prod_{k=1}^{(p-1)/2} (\zeta^{2k-1} - \zeta^{-(2k-1)}) = \begin{cases} \varepsilon \sqrt{p} & \text{falls } p \equiv 1(4), \\ \varepsilon i \sqrt{p} & \text{falls } p \equiv 3(4). \end{cases} \end{aligned}$$

mit $\varepsilon = \pm 1$.

Wir wollen $\varepsilon = 1$ zeigen. Dazu betrachten wir das Polynom

$$f(x) = \sum_{j=1}^{p-1} \chi(j)x^j - \varepsilon \prod_{k=1}^{(p-1)/2} (x^{2k-1} - x^{p-(2k-1)}) \in \mathbb{Z}[x].$$

Man hat $f(\zeta) = g(\chi) - g(\chi) = 0$ und $f(1) = \sum_{j=1}^{p-1} \chi(j) = 0$. Die Körpererweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$ hat den Grad $p-1$ und das Minimalpolynom von ζ ist $1 + x + \dots + x^{p-1}$. Es teilt $f(x)$ wegen $f(\zeta) = 0$:

$$1 + x + \dots + x^p \mid f(x).$$

Wegen $f(1) = 0$ gilt auch $x-1 \mid f(x)$. Da aber $x-1$ und $1+x+\dots+x^{p-1}$ relativ prim sind, ist auch ihr Produkt x^p-1 ein Teiler von f :

$$x^p - 1 \mid f(x).$$

Also kann man $f(x) = (x^p - 1)h(x)$ mit einem $h \in \mathbb{Z}[x]$ schreiben. Setzen wir $x = e^z$ ein, so folgt

$$\begin{aligned} f(e^z) &= (e^{pz} - 1)h(e^z) \\ &= \sum_{j=1}^{p-1} \chi(j)e^{jz} - \varepsilon \prod_{k=1}^{(p-1)/2} (e^{(2k-1)z} - e^{(p-(2k-1))z}). \end{aligned}$$

Setzt man darin $e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$ ein, und vergleicht die Koeffizienten von $z^{(p-1)/2}$ auf beiden Seiten, so erhält man

$$\frac{pA}{B} = \sum_{j=1}^{p-1} \frac{\chi(j)j^{(p-1)/2}}{\left(\frac{p-1}{2}\right)!} - \varepsilon \prod_{k=1}^{(p-1)/2} (4k - p - 2);$$

dabei ist die linke Seite der Koeffizient von $z^{(p-1)/2}$ in $(e^{pz} - 1)h(e^z)$, und die rechte Seite der Koeffizient von $z^{(p-1)/2}$ der anderen Seite oben. Man hat $A, B \in \mathbb{Z}$ mit $p \nmid B$, siehe [10], Seite 78. Nun multipliziert man die obige Gleichung mit $B \left(\frac{p-1}{2}\right)!$ durch und betrachtet sie modulo p . Dann ist die linke Seite kongruent Null. Wegen $p \nmid B$ kann man dann das B wieder kürzen und erhält

$$\begin{aligned} \sum_{j=1}^{p-1} \chi(j)j^{(p-1)/2} &\equiv \varepsilon \left(\frac{p-1}{2}\right)! \prod_{k=1}^{(p-1)/2} (4k - 2) \\ &\equiv \varepsilon \cdot 2 \cdot 4 \cdot 6 \cdots (p-1) \prod_{k=1}^{(p-1)/2} (2k - 1) \\ &\equiv \varepsilon(p-1)! \\ &\equiv -\varepsilon. \end{aligned}$$

Im letzten Schritt haben wir Wilsons Satz benutzt. Andererseits gilt aber $j^{(p-1)/2} \equiv \chi(j) \pmod{p}$ nach Theorem 2.6.5, also

$$-\varepsilon \equiv \sum_{j=1}^{p-1} \chi(j)j^{(p-1)/2} \equiv \sum_{j=1}^{p-1} \chi(j)^2 \equiv p-1 \pmod{p},$$

also $\varepsilon \equiv 1 \pmod{p}$. Wegen $\varepsilon = \pm 1$ folgt $\varepsilon = 1$ und wir sind endlich fertig. \square

2.7. Kubische Gauß-Summen

Es sei $\omega = e^{2\pi i/3} = \frac{\sqrt{-3}-1}{2}$ eine dritte EW. Offensichtlich ist ω Nullstelle von $x^3 - 1 = (x-1)(x^2+x+1)$ und erfüllt daher

$$(2.23) \quad 0 = 1 + \omega + \omega^2$$

$$(2.24) \quad \bar{\omega} = \omega^{-1} = \omega^2.$$

Die Menge $D = \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ ist ein Unterring der komplexen Zahlen, da sie unter Multiplikation abgeschlossen ist. Mit (2.23) gilt nämlich

$$\begin{aligned} (a + b\omega)(c + d\omega) &= ac + (ad + bc)\omega + bd\omega^2 \\ &= (ac - bd) + (ad + bc - bd)\omega \end{aligned}$$

Dieser Ring ist auch abgeschlossen unter komplexer Konjugation:

$$\overline{a + b\omega} = a + b\bar{\omega} = a + b\omega^2 = (a - b) - b\omega.$$

DEFINITION 2.7.1. Ein Integritätsring R heißt *Euklidisch*, falls es eine Funktion $\lambda: R \setminus 0 \rightarrow \mathbb{N} \cup 0$ gibt, so daß für alle $a, b \in R$, $b \neq 0$ Elemente $c, d \in R$ existieren mit $a = cb + d$, wobei entweder $d = 0$ oder $\lambda(d) < \lambda(b)$ gilt.

BEISPIEL 2.7.2. Die Ringe \mathbb{Z} , $K[x]$, $\mathbb{Z}[i]$ und die Ganzheitsringe \mathcal{O}_d in $\mathbb{Q}(\sqrt{d})$ für $d = -1, -2, -3, -7, -11$ sind Euklidisch, siehe Abschnitt 1.1.

In der Tat ist $\mathcal{O}_d = \mathbb{Z}[i]$ für $d = -1$ und $\mathcal{O}_d = \mathbb{Z}[\omega]$ für $d = -3$. Bekanntlich ist jeder Euklidische Ring auch ein HIR (Hauptidealring), und jeder HIR ein faktorieller Ring. Die Umkehrungen gelten i.a. nicht: $\mathbb{Z}[x]$ ist zwar faktoriell aber kein HIR. Und \mathcal{O}_{-19} ist ein HIR, aber kein (Norm)-Euklidischer Ring. Wir wollen hier folgenden Satz beweisen:

SATZ 2.7.3. $D = \mathbb{Z}[\omega]$ ist ein Euklidischer Ring.

BEWEIS. Sei $\alpha = a + b\omega \in \mathbb{Z}[\omega]$. Die Norm $N(\alpha)$ ist definiert durch

$$N(\alpha) = \alpha\bar{\alpha} = (a + b\omega)(a + b\bar{\omega}) = a^2 - ab + b^2.$$

Wir wählen $\lambda(\alpha) = N(\alpha)$. Seien also $\alpha, \beta \in \mathbb{Z}[\omega]$ mit $\beta \neq 0$. Dann ist $\beta\bar{\beta} > 0$ und $\alpha\bar{\beta} \in \mathbb{Z}[\omega]$, und

$$\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{\beta\bar{\beta}} = r + s\omega,$$

mit $r, s \in \mathbb{Q}$. Nun wähle man $m, n \in \mathbb{Z}$ mit $|r - m| \leq 1/2$ und $|s - n| \leq 1/2$. Dann setzt man $\gamma = m + n\omega$ und rechnet

$$\begin{aligned} \lambda\left(\frac{\alpha}{\beta} - \gamma\right) &= N(r - m + (s - n)\omega) \\ &= (r - m)^2 - (r - m)(s - n) + (s - n)^2 \\ &\leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} < 1. \end{aligned}$$

Mit $\delta = \alpha - \gamma\beta$ gilt deshalb entweder $\delta = 0$ oder

$$\lambda(\delta) = \lambda\left(\beta\left(\frac{\alpha}{\beta} - \gamma\right)\right) = \lambda(\beta)\lambda\left(\frac{\alpha}{\beta} - \gamma\right) < \lambda(\beta).$$

□

SATZ 2.7.4. *Die Einheiten in $D = \mathbb{Z}[\omega]$ sind genau die Elemente*

$$1, -1, \omega, -\omega, \omega^2, -\omega^2.$$

BEWEIS. Zunächst ist $\alpha \in D$ genau dann eine Einheit, wenn $N(\alpha) = 1$ gilt. Ist nämlich $N(\alpha) = 1$, so hat man $\alpha\bar{\alpha} = 1$ mit $\bar{\alpha} \in D$, also ist α eine Einheit. Ist α umgekehrt eine Einheit, so gibt es ein $\beta \in D$ mit $\alpha\beta = 1$, also mit $N(\alpha)N(\beta) = N(1) = 1$. Diese Gleichung hat über \mathbb{N} nur die Lösung $N(\alpha) = N(\beta) = 1$.

Sei nun $\alpha = a + b\omega$ eine Einheit, d.h.,

$$1 = N(\alpha) = a^2 - ab + b^2 = \frac{3b^2 + (2a - b)^2}{4}.$$

Die diophantische Gleichung $(2a - b)^2 + 3b^2 = 4$ hat aber nur die Lösungen $2a - b = \pm 1, b = \pm 1$, oder $2a - b = \pm 2, b = 0$. Das ergibt 6 Möglichkeiten: $1, -1, \omega, -\omega, -1 - \omega, 1 + \omega$. Wegen $-1 - \omega = \omega^2$ und $1 + \omega = -\omega^2$ ist das die Behauptung. □

Welche Elemente $\alpha \in D$ sind nun prim? Betrachten wir zunächst die rationalen Primzahlen $p \in \mathbb{P}$. Sie bleiben nicht notwendigerweise prim in D , wie das folgende Beispiel zeigt:

$$7 = 6 - \omega - \omega^2 = (3 + \omega)(2 - \omega).$$

Es gilt folgendes Resultat.

LEMMA 2.7.5. *Ist π ein Primelement in D , so gibt es ein $p \in \mathbb{P}$ mit $N(\pi) = p$ oder $N(\pi) = p^2$. Im letzteren Fall sind π und p assoziiert, im ersteren Fall nicht. Gilt umgekehrt $N(\pi) = p$ mit $p \in \mathbb{P}$, so ist π prim in D .*

BEWEIS. Da π keine Einheit ist, gilt $\pi\bar{\pi} = n > 1$. Also gibt es ein $p \in \mathbb{P}$ mit $p \mid n$, also $\pi \mid p$. Dann schreibt man $p = \pi\gamma$ mit $\gamma \in D$ und erhält $p^2 = N(p) = N(\pi)N(\gamma)$. Diese Gleichung hat zwei Lösungen. Entweder ist $N(\pi) = p^2, N(\gamma) = 1$, also γ eine Einheit, oder $N(\pi) = N(\gamma) = p$. Dann ist π zu keiner rationalen Primzahl q assoziiert. Angenommen, man hätte doch $\pi = \varepsilon q$, ε Einheit, dann wäre

$$p = N(\pi) = N(\varepsilon)N(q) = q^2,$$

was offensichtlich unmöglich ist. Um die letzte Aussage zu zeigen, nehme man an, daß $\pi = \rho\gamma$ nicht prim wäre. Dann wären $N(\rho), N(\gamma) > 1$, und $p = N(\pi) = N(\rho)N(\gamma)$, und damit p nicht prim, Widerspruch. □

SATZ 2.7.6. *Seien p und q rationale Primzahlen. Dann gilt:*

- (1) *Ist $q \equiv 2(3)$, so ist q prim in D .*
- (2) *Ist $p \equiv 1(3)$, so ist $p = N(\pi) = \pi\bar{\pi}$ mit einem Primelement $\pi \in D$.*
- (3) *Die Zahl 3 zerlegt sich als $3 = -\omega^2(1 - \omega)^2$, wobei $1 - \omega$ prim ist in D .*

BEWEIS. Zu (1): wäre q nicht prim, hätte man $q = \pi\gamma$ mit $N(\pi), N(\gamma) > 1$. Dann wäre $q^2 = N(q) = N(\pi)N(\gamma)$, also $N(\pi) = q$. Sei $\pi = a + b\omega$. Dann folgte

$$\begin{aligned} q &= N(\pi) = a^2 - ab + b^2, \\ 4q &= (2a - b)^2 + 3b^2. \end{aligned}$$

Damit wäre $q \equiv (2a - b)^2 \equiv 2 \pmod{3}$. Es gibt aber kein Quadrat, welches kongruent 2 modulo 3 wäre, Widerspruch.

Zu (2): mit dem quadratischen Reziprozitätsgesetz folgt

$$\begin{aligned} \left(\frac{-3}{p}\right) &= \left(\frac{-1}{p}\right) \left(\frac{3}{p}\right) = (-1)^{(p-1)/2} (-1)^{\frac{p-1}{2} \frac{3-1}{2}} \left(\frac{p}{3}\right) \\ &= \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1, \end{aligned}$$

weil ja $p \equiv 1(3)$. Also gibt es ein $a \in \mathbb{Z}$ mit $a^2 \equiv -3(p)$, also

$$pb = a^2 + 3 = (a + 1 + 2\omega)(a - 1 - 2\omega)$$

für ein $b \in \mathbb{Z}$. Da D ein faktorieller Ring ist, gilt: wäre p prim in D , so müßte es einen der beiden Faktoren teilen:

$$p \mid (a + 1 + 2\omega) \quad \text{oder} \quad p \mid (a - 1 - 2\omega).$$

Ohne Einschränkung sei $\gamma p = a + 1 + 2\omega$. Dann gibt es $c, d \in \mathbb{Z}$ mit $\gamma = c + d\omega$ und

$$cp - a - 1 + \omega(dp - 2) = 0,$$

also $dp = 2$. Da aber $p > 2$, ist das ein Widerspruch. Also ist p nicht prim in D und hat eine echte Zerlegung $p = \pi\gamma$ mit $N(\pi), N(\gamma) > 1$. Damit ist $p^2 = N(\pi)N(\gamma)$ und $p = N(\pi) = \pi\bar{\pi}$.

Zu (3): Wegen $x^3 - 1 = (x - 1)(x - \omega)(x - \omega^2)$ gilt

$$\begin{aligned} x^2 + x + 1 &= (x - \omega)(x - \omega^2), \\ 3 &= (1 - \omega)(1 - \omega^2) = (1 + \omega)(1 - \omega)^2 = -\omega^2(1 - \omega)^2 \\ 9 &= N(-\omega^2)N((1 - \omega)^2) = (N(1 - \omega))^2. \end{aligned}$$

Damit gilt $N(1 - \omega) = 3$ und $1 - \omega$ ist prim nach Lemma 2.7.5. □

Für ein $\gamma \neq 0$, das keine Einheit ist, betrachten wir den Restklassenring $D/\gamma D$. Die Äquivalenzrelation ist gegeben durch

$$\alpha \equiv \beta(\gamma) \iff \gamma \mid (\alpha - \beta).$$

Aus der algebraischen Zahlentheorie wissen wir:

THEOREM 2.7.7. *Sei \mathcal{O} der Ring der ganzen Zahlen eines Zahlkörpers und I ein Ideal in \mathcal{O} . Dann ist \mathcal{O}/I ein endlicher Ring mit $N(I)$ Elementen.*

Natürlich ist \mathcal{O}/I ein endlicher Körper, wenn I prim ist.

KOROLLAR 2.7.8. Sei $\pi \in D$ ein Primelement. Dann ist $D/\pi D$ ein endlicher Körper mit $N(\pi)$ Elementen.

Für ein Primelement π in D hat die multiplikative Gruppe von $D/\pi D$ genau $N(\pi) - 1$ Elemente. Der Satz von Euler besagt, für $\bar{\alpha} = \alpha \bmod \pi \in D/\pi D$:

$$\bar{\alpha}^{N(\pi)-1} = \bar{1}.$$

Wir haben folgendes Resultat:

LEMMA 2.7.9. Für $\pi \in D$ prim und $\alpha \in D$ mit $\pi \nmid \alpha$ gilt

$$\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}.$$

Ferner gilt $N(\pi) = 3$ oder $N(\pi) \equiv 1(3)$.

BEWEIS. Es sei $N(\pi) \neq 3$. Dann sind $\bar{1}, \bar{\omega}, \bar{\omega}^2$ alle verschieden in $D/\pi D$. In der Tat, wäre etwa $\bar{1} = \bar{\omega}$, so hätte man $\pi \mid (1 - \omega)$. Wegen Satz 2.7.6 ist $1 - \omega$ prim, und damit π und $1 - \omega$ assoziiert. Es folgt $N(\pi) = N(1 - \omega) = 3$, Widerspruch. Also ist $U = \{\bar{1}, \bar{\omega}, \bar{\omega}^2\}$ eine Untergruppe der Ordnung 3 in $((D/\pi D)^*, \cdot)$. Nach Lagrange gilt $3 \mid N(\pi) - 1$, also $N(\pi) \equiv 1(3)$. \square

LEMMA 2.7.10. Sei $\pi \in D$ prim, $N(\pi) \neq 3$ und $\alpha \in D$ mit $\pi \nmid \alpha$. Dann gibt es ein eindeutig bestimmtes $m \in \{0, 1, 2\}$ mit

$$(2.25) \quad \alpha^{\frac{N(\pi)-1}{3}} \equiv \omega^m \pmod{\pi}.$$

BEWEIS. Wegen Lemma 2.7.9 gilt $\pi \mid \alpha^{N(\pi)-1} - 1$. Es gilt

$$\alpha^{N(\pi)-1} - 1 = \left(\alpha^{\frac{N(\pi)-1}{3}} - 1 \right) \left(\alpha^{\frac{N(\pi)-1}{3}} - \omega \right) \left(\alpha^{\frac{N(\pi)-1}{3}} - \omega^2 \right).$$

Da π prim ist und die linke Seite teilt, muß π auch einen Faktor auf der rechten Seite teilen. Man sieht leicht, daß π genau einen der drei Faktoren teilt. Würde π zwei Faktoren teilen, etwa die beiden ersten, dann auch ihre Differenz: $\pi \mid 1 - \omega$. Das ist ein Widerspruch zu $N(\pi) \neq 3$. \square

Nun können wir endlich den kubischen Charakter $\chi_\pi(\alpha) = \left(\frac{\alpha}{\pi}\right)_3$ definieren.

DEFINITION 2.7.11. Sei $\pi \in D$ prim und $N(\pi) \neq 3$. Der kubische Charakter von α modulo π ist definiert durch

$$\begin{aligned} \left(\frac{\alpha}{\pi}\right)_3 &= 0, & \text{falls } \pi \mid \alpha, \\ \left(\frac{\alpha}{\pi}\right)_3 &\equiv \alpha^{\frac{N(\pi)-1}{3}} \pmod{\pi}, & \text{falls } \pi \nmid \alpha, \end{aligned}$$

wobei $\left(\frac{\alpha}{\pi}\right)_3 \in \{1, \omega, \omega^2\}$ im zweiten Fall nach Lemma 2.7.10 eindeutig bestimmt ist.

SATZ 2.7.12. Der kubische Charakter hat folgende Eigenschaften:

(1) $\left(\frac{\alpha}{\pi}\right)_3 = 1$ genau dann wenn $x^3 \equiv \alpha \pmod{\pi}$ lösbar ist.

(2) $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$.

(3) Aus $\alpha \equiv \beta \pmod{\pi}$ folgt $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$.

BEWEIS. Zu (1): Für einen endlichen Körper F und ein $\alpha \in F^\times$ gilt: $x^n = \alpha$ hat in F^\times genau dann Lösungen, wenn $\alpha^{(q-1)/d} = 1$ ist, wobei $|F^\times| = q - 1$ und $d = (n, q - 1)$. Mit $F = D/\pi D$, $q = N(\pi)$ und $n = 3$ heißt das also: $x^3 \equiv \alpha \pmod{\pi}$ ist genau dann lösbar, wenn

$$\left(\frac{\alpha}{\pi}\right)_3 = \alpha^{(q-1)/d} = \alpha^{(N(\pi)-1)/3} \equiv 1 \pmod{\pi}$$

gilt, wobei $d = (3, N(\pi) - 1) = 3$.

Zu (2):

$$\left(\frac{\alpha\beta}{\pi}\right)_3 \equiv (\alpha\beta)^{(N(\pi)-1)/3} \equiv \alpha^{(N(\pi)-1)/3} \beta^{(N(\pi)-1)/3} \equiv \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3.$$

Zu (3): Aus $\alpha \equiv \beta \pmod{\pi}$ folgt

$$\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{(N(\pi)-1)/3} \equiv \beta^{(N(\pi)-1)/3} \equiv \left(\frac{\beta}{\pi}\right)_3,$$

und deshalb die Behauptung. □

Im Gegensatz zum Ring $\mathbb{Z}[i]$ hat hier jedes $\alpha \in D^\times$ sechs Assoziierte. Wir beseitigen die Mehrdeutigkeit wie folgt:

DEFINITION 2.7.13. Sei $\pi \in D$ prim. Dann heißt π *primär*, falls $\pi \equiv 2 \pmod{3}$ ist.

Ist $\pi = q$ rational, so ist π automatisch primär, siehe Satz 2.7.6. Ansonsten, für $\pi = a + b\omega$ bedeutet das $3 \mid (a - 2 + b\omega)$, also

$$a \equiv 2(3), \quad b \equiv 0(3).$$

SATZ 2.7.14. Für $\pi \in D$ gelte $N(\pi) = p \equiv 1(3)$ mit einer rationalen Primzahl p . Dann ist π prim in D und genau eines seiner sechs Assoziierten primär.

Ein Beweis findet sich in [10], Prop. 9.3.5.

BEISPIEL 2.7.15. Das ist Element $\pi = 3 + \omega$ ist prim in D , und $-\omega^2(3 + \omega) = 2 + 3\omega$ ist primär.

Wegen $N(\pi) = N(3 + \omega) = 7$ ist π prim. Offenbar sind die fünf Assoziierten $\pi, \omega\pi, -\pi, -\omega\pi, \omega^2\pi$ nicht primär. Dagegen ist $-\omega^2(3 + \omega)$ primär.

Analog zum quadratischen Reziprozitätsgesetz gibt es auch ein kubisches, siehe [10]:

THEOREM 2.7.16. *Es seien π_1, π_2 primäre Elemente in D mit $N(\pi_1) \neq N(\pi_2)$, sowie beide Normen von 3 verschieden. Dann gilt*

$$\left(\frac{\pi_2}{\pi_1}\right)_3 = \left(\frac{\pi_1}{\pi_2}\right)_3.$$

Im Beweis werden Jacobi-Summen zum Charakter $\chi_\pi(\alpha) = \left(\frac{\alpha}{\pi}\right)_3$ verwendet.

DEFINITION 2.7.17. Es seien χ, ψ zwei Dirichlet-Charaktere modulo $p \in \mathbb{P}$. Die *Jacobi-Summe* zu χ und ψ ist definiert durch

$$J(\chi, \psi) = \sum_{a \bmod p} \chi(a)\psi(1-a).$$

Jacobi-Summen lassen sich in gewissen Fällen durch Gauß-Summen ausdrücken. Sind χ, ψ und $\chi\psi$ nicht-trivial, so gilt

$$J(\chi, \psi) = \frac{g(\chi)g(\psi)}{g(\chi\psi)}.$$

Es gilt das folgende Lemma, das wir später noch brauchen.

LEMMA 2.7.18. *Sei $\pi \in D$ primär. Dann gilt $J(\chi_\pi, \chi_\pi) = \pi$.*

2.8. Die Kummersche Vermutung

Sei χ ein Dirichlet-Charakter modulo $p \in \mathbb{P}$ der Ordnung n . Da die Charaktergruppe $(\mathbb{Z}/p\mathbb{Z})^*$ zyklisch der Ordnung $p-1$ ist, kann man ein Element der Ordnung n nur haben, wenn $n \mid p-1$ gilt. Fixieren wir also ein $n \geq 2$ und eine Primzahl p mit $p \equiv 1(n)$. Wir erinnern uns daran, daß die Gauß-Summe $g(\chi)$ den Absolutbetrag \sqrt{p} hat für alle n . Es gilt also

$$(2.26) \quad |g(\chi)^n| = |g(\chi)|^n = p^{n/2}, \quad n \geq 2.$$

Andererseits ist die komplexe Zahl $g(\chi)^n$ als Zahl des Einheitswurzelkörpers $\mathbb{Q}[\zeta_n]$ algebraisch bekannt, und die Zahl $g(\chi)$ aus dem Körperkompositum

$\mathbb{Q}[\zeta_n]\mathbb{Q}[\zeta_p]$ genau n -deutig bestimmt. Man kann leicht zeigen, daß

$$(2.27) \quad g(\chi)^n = \begin{cases} \chi(-1)pJ(\chi, \chi)J(\chi, \chi^2) \cdots J(\chi, \chi^{n-2}) & \text{falls } n \geq 3, \\ \chi(-1)p & \text{falls } n = 2. \end{cases}$$

Damit liegt die komplexe Zahl $g(\chi)$ also auf dem Kreis $\{z \in \mathbb{C} \mid |z| = \sqrt{p}\}$ und ist bis auf eine n -te EW bestimmt.

Kummer fragte sich, welches Argument diese Zahl hat, in Abhängigkeit von p , welches die Primzahlen $p \equiv 1(n)$ durchläuft, und bei fixiertem $n \geq 2$. In der Tat, für $n = 2$ kennen wir die Antwort schon. (2.26) und (2.27) besagen, daß die Zahl $g(\chi)$ eine der beiden Wurzeln des Polynoms $x^2 - (-1)^{(p-1)/2}p$ ist. Für $p \equiv 1(4)$ hat man also \sqrt{p} oder $-\sqrt{p}$ zur Auswahl; und für $p \equiv 3(4)$ hat man $i\sqrt{p}$ oder $-i\sqrt{p}$ zur Auswahl. Nach Theorem 2.6.12 von Gauß hat man immer das positive Vorzeichen, und das völlig unabhängig von der Primzahl $p > 2$.

Für $n = 3$ wird die Frage von Kummer schwer. Trotzdem wollen wir uns jetzt mit dem Argument der kubischen Gauß-Summe beschäftigen. Sei π prim in $D = \mathbb{Z}[\omega]$, mit $N(\pi) = p \equiv 1(3)$. Weiterhin sei $\chi_\pi(\alpha) = \left(\frac{\alpha}{\pi}\right)_3$ und

$$g(\pi) := g(\chi_\pi) = G(1, \chi_\pi)$$

die Gauß-Summe zu χ_π . Wegen (2.26) und (2.27) gilt

$$(2.28) \quad g(\pi)^3 = p\pi, \quad |g(\pi)^3| = p^{3/2}.$$

In der Tat, (2.27) besagt $g(\pi)^3 = \chi_\pi(-1)pJ(\chi_\pi, \chi_\pi)$, und es ist

$$\chi_\pi(-1) = \chi_\pi((-1)^3) = (\chi_\pi(-1))^3 = 1,$$

da χ_π ein kubischer Charakter ist. Weiterhin ist $J(\chi_\pi, \chi_\pi) = \pi$ wegen Lemma 2.7.18. Man kann $g(\pi)$ noch normieren.

DEFINITION 2.8.1. Die Gauß-Summe

$$h(\pi) = \frac{g(\pi)}{\sqrt{p}} = \frac{g(\pi)}{\sqrt{N(\pi)}}$$

heißt normierte kubische Gauß-Summe. Sie liegt auf dem Einheitskreis in \mathbb{C} :

$$(2.29) \quad |h(\pi)^3| = 1.$$

Wir wollen neben der komplexen Zahl $g(\pi)$ auch noch die reelle Zahl $\text{Re}(g(\pi))$ untersuchen.

LEMMA 2.8.2. *Es sei $\gamma = 2\text{Re}(g(\pi)) = g(\pi) + \overline{g(\pi)}$. Dann gilt*

$$\gamma = \sum_{r=0}^{p-1} \cos\left(\frac{2\pi r^3}{p}\right).$$

BEWEIS.

$$\begin{aligned}\gamma &= g(\chi_\pi) + \chi_\pi(-1)\overline{g(\chi_\pi)} = g(\chi_\pi) + g(\overline{\chi_\pi}) \\ &= g(\chi_\pi) + g(\chi_\pi^2).\end{aligned}$$

Nun benutzen wir folgendes Resultat für kubische Charaktere (siehe [10]):

$$(2.30) \quad \sum_{r=0}^{p-1} \zeta_p^{r^3} = g(\chi) + g(\chi^2).$$

Dann erhalten wir, weil γ reell ist

$$\begin{aligned}\gamma &= g(\chi_\pi) + g(\chi_\pi^2) = \sum_{r=0}^{p-1} e^{2\pi i r^3/p} \\ &= \sum_{r=0}^{p-1} \cos\left(\frac{2\pi r^3}{p}\right) + \sum_{r=0}^{p-1} i \sin\left(\frac{2\pi r^3}{p}\right) \\ &= \sum_{r=0}^{p-1} \cos\left(\frac{2\pi r^3}{p}\right).\end{aligned}$$

□

Nun sehen wir, welche Möglichkeiten es für die reelle Zahl $\gamma = 2\operatorname{Re}(g(\pi))$ gibt.

LEMMA 2.8.3. *Es sei $\pi = a + b\omega \in D$. Dann ist γ eine reelle Wurzel des Polynoms $x^3 - 3px - (2a - b)p$.*

BEWEIS. Mit (2.28) folgt

$$\begin{aligned}\gamma^3 &= (g(\pi) + \overline{g(\pi)})^3 = g(\pi)^3 + 3g(\pi)\overline{g(\pi)}(g(\pi) + \overline{g(\pi)}) + (\overline{g(\pi)})^3 \\ &= p\pi + 3|g(\pi)|^2\gamma + p\overline{\pi} \\ &= p\pi + 3p\gamma + p\overline{\pi} \\ &= p(a + b\omega + a + b\overline{\omega}) + 3p\gamma \\ &= p(2a - b) + 3p\gamma.\end{aligned}$$

□

Die komplexe Zahl $g(\pi)$ ist ja nun durch (2.28) bis auf eine Kubikwurzel $1, \omega, \omega^2$ bestimmt. Kummer fragte sich nun, welche Kubikwurzel man nehmen müsse, in Abhängigkeit von Primelementen $\pi \in D$ mit $N(\pi) = p \equiv 1(3)$. Er fand keine Regel, um $g(\pi)$ mit Hilfe von *Kongruenzbedingungen* an π zu bestimmen. Für quadratische Gauß-Summen ist das ja möglich. Dort hängt der Wert der Gauß-Summe ja in der Tat von Kongruenzbedingungen an p ab. Kummer wertete $g(\pi)$ deshalb für viele π numerisch aus, um zumindest eine gewisse Statistik zu erhalten. Er tat das, indem er die Primelemente π in *drei Klassen* C_1, C_2, C_3 einteilte, je

nachdem, ob für die reelle Zahl $\gamma = 2\operatorname{Re}(g(\pi))$ gilt

$$C_1 : -2\sqrt{p} < \gamma < -\sqrt{p}$$

$$C_2 : -\sqrt{p} < \gamma < \sqrt{p}$$

$$C_3 : \sqrt{p} < \gamma < 2\sqrt{p}$$

Wegen Lemma 2.8.3 tritt auch genau einer dieser drei Fälle auf: die Wurzeln von $x^3 - 3px - (2a - b)p$ sind $\gamma = 2\operatorname{Re}(g(\pi))$, $2\operatorname{Re}(\omega g(\pi))$ und $2\operatorname{Re}(\omega^2 g(\pi))$. Indem man $|g(\pi)| = \sqrt{p}$ benutzt, kann man leicht sehen, daß jedes Intervall $(-2\sqrt{p}, -\sqrt{p})$, $(-\sqrt{p}, \sqrt{p})$ und $(\sqrt{p}, 2\sqrt{p})$ genau eine der drei Wurzeln des Polynoms $x^3 - 3px - (2a - b)p$ enthält.

Kummer betrachtete für $j = 1, 2, 3$ die Zahlen

$$N_j(x) = \#\{\pi \in D, N(\pi) = p \equiv 1(3) \mid N(\pi) \leq x, \gamma \in C_j\}.$$

Er fand für $x = 500$ die folgenden Werte:

$$N_1(500) = 7, N_2(500) = 14, N_3(500) = 24.$$

Die Verhältnisse $7 : 14 : 24$ sind ungefähr wie $1 : 2 : 3$. Kummer vermutete eine asymptotische Verteilung, also für $x \rightarrow \infty$, in diesem Verhältnis. Hasse jedenfalls sprach von der *Kummer-Vermutung*. Allerdings fanden J. von Neumann und H.H. Goldstine 1953 folgende Verteilung:

$$N_1(10000) = 138, N_2(10000) = 201, N_3(10000) = 272.$$

Das verhält sich eher wie $2 : 3 : 4$. Nachdem E. Lehmer ein Verhältnis von ungefähr $3 : 4 : 5$ entdeckte, kam der Verdacht auf, daß die Werte von γ asymptotisch *gleichverteilt* in den drei Intervallen liegen könnten. Tatsächlich bewiesen dies Heath-Brown und Patterson 1978, siehe [9]:

THEOREM 2.8.4. *Für $\pi \in D$ prim mit $\pi \equiv 1(3)$ sind die Zahlen $h(\pi)$ auf dem Einheitskreis gleichverteilt, in folgendem Sinne: es existiert eine absolute Konstante $A > 0$, so daß für alle Winkel $0 \leq \theta_1 \leq \theta_2 \leq 2\pi$ gilt*

$$\sum_{\substack{N(\pi) \leq x \\ \theta_1 < \arg(h(\pi)) \leq \theta_2}} 1 = \frac{\theta_2 - \theta_1}{2\pi} \operatorname{li}(x) + O\left(x \exp\left(-A\sqrt{\log(x)}\right)\right).$$

Im Beweis wird u.a. der verallgemeinerte Primzahlsatz benutzt. Der gewöhnliche besagt ja

$$\pi(x) = \sum_{p \leq x} 1 = \operatorname{li}(x) + O\left(x \exp\left(-A\sqrt{\log(x)}\right)\right)$$

für ein $A > 0$.

BEMERKUNG 2.8.5. Man beachte, daß dieses Resultat keine Einsicht darüber erlaubt, wie man eine individuelle Gauß-Summe $g(\pi)$ wirklich bestimmt. Dazu gibt es eine explizite Formel, siehe [12], die $g(\pi)$ als Produkt von Divisionswerten einer elliptischen Funktion darstellt. Dabei tritt die Weierstrass \wp -Funktion auf.

2.9. Primzahlen in arithmetischen Progressionen

Der Satz von Dirichlet, den wir hier beweisen wollen, besagt, daß jede Folge $a(n) = kn + h$ mit $(k, h) = 1$ unendlich viele Primzahlen enthält. Nehmen wir etwa $a(n) = 2n + 1$. Dort ist die Aussage klar. Für $a(n) = 4n \pm 1$ ist das schon weniger offensichtlich. Man kann es aber immerhin elementar beweisen.

BEISPIEL 2.9.1. *Es gibt unendlich viele Primzahlen der Form $4n - 1$ bzw. der Form $4n + 1$.*

Angenommen, es gäbe nur endlich viele Primzahlen $\{p_1, \dots, p_r\}$ der Form $4n - 1$. Dann betrachte man $N = 4p_1 \cdots p_r - 1$. Die Primfaktoren von N können nicht alle kongruent 1 modulo 4 sein, sonst wäre es auch N , wegen

$$(4a + 1)(4b + 1) = 4(4ab + a + b) + 1.$$

Also gibt es ein $p \mid N$ mit $p \equiv -1(4)$. Es ist aber offensichtlich von allen p_i verschieden nach Konstruktion von N . Widerspruch.

Zur zweiten Behauptung. Angenommen, es gäbe nur endlich viele Primzahlen $\{p_1, \dots, p_r\}$ der Form $4n + 1$. Dann betrachte man $N = 4(p_1 \cdots p_r)^2 + 1$. Angenommen $p \mid N$. Das heie

$$4(p_1 \cdots p_r)^2 + 1 \equiv 0(p).$$

Somit wre -1 ein quadratischer Rest modulo p , also

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = 1,$$

und damit $p \equiv 1(4)$. Wegen $p \neq p_i$ ist das ein Widerspruch.

Diese elementaren Beweise gibt es fr $a(n) = kn + h$ aber nur dann, wenn $h^2 \equiv 1(k)$ ist. Fr $a(n) = 7n + 2$ funktioniert das also zum Beispiel nicht. Auerdem ist es ja nicht wnschenswert, fr jeden Fall einen anderen Beweis zu haben. Dirichlets Beweis funktioniert fr jeden Fall. Das Resultat, das wir beweisen wollen, ist wie folgt.

THEOREM 2.9.2 (Dirichlet). *Mit $k > 0$ und $(h, k) = 1$ gilt fr alle $x > 1$*

$$(2.31) \quad \sum_{\substack{p \leq x \\ p \equiv h(k)}} \frac{\log(p)}{p} = \frac{1}{\varphi(k)} \log(x) + O(1).$$

Inbesondere gibt es unendlich viele Primzahlen $p \equiv h(k)$.

Der zweite Teil folgt aus (2.31) fr $x \rightarrow \infty$. Zum Beweis bentigen wir einige Lemmata. Kommen wir zuerst noch einmal auf Satz 1.3.23 zurck. Seien f, g zwei arithmetische Funktionen. Fr $h = f * g$ setze man $H(x) = \sum_{n \leq x} h(n)$, $F(x) = \sum_{n \leq x} f(n)$ und $G(x) = \sum_{n \leq x} g(n)$. Dann gilt

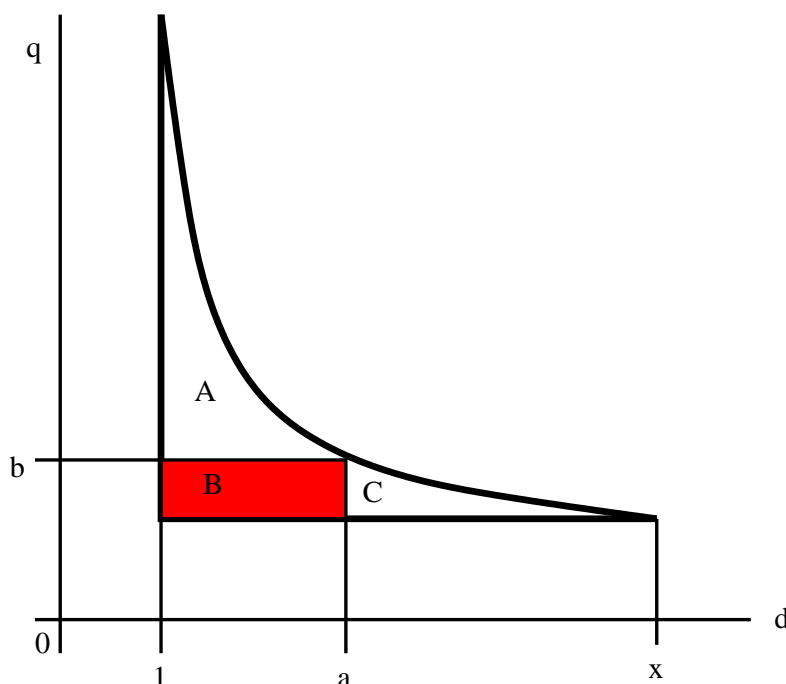
$$\begin{aligned} H(x) &= \sum_{n \leq x} f(n)G\left(\frac{x}{n}\right) = \sum_{n \leq x} g(n)F\left(\frac{x}{n}\right) \\ &= \sum_{n \leq x} \sum_{d \mid n} f(d)g\left(\frac{n}{d}\right) = \sum_{\substack{q, d \\ qd \leq x}} f(d)g(q). \end{aligned}$$

Mit diesen Bezeichnungen gilt folgendes allgemeineres Resultat:

SATZ 2.9.3. Für positive reelle Zahlen a, b mit $ab = x$ gilt

$$\sum_{\substack{q,d \\ qd \leq x}} f(d)g(q) = \sum_{n \leq a} f(n)G\left(\frac{x}{n}\right) + \sum_{n \leq b} g(n)F\left(\frac{x}{n}\right) - F(a)G(b).$$

BEWEIS. Betrachten wir die Gitterpunkte (q, d) in folgender Zeichnung.



Auf der linken Seite unserer Gleichung summieren wir über alle Gitterpunkte unter der Hyperbel $qd = x$, d.h., in der Region $A \cup B \cup C$. Auf der rechten Seite spalten wir die Summe aber in zwei Teile: einen vertikalen und einen horizontalen. Mit anderen Worten, wir summieren dort über die Gitterpunkte in $A \cup B$, und dann über die Gitterpunkte in $B \cup C$, und ziehen die Summe von denen in B wieder ab, weil wir sie doppelt gezählt haben:

$$\begin{aligned} H(x) &= \sum_{d \leq a} \sum_{q \leq x/d} f(d)g(q) + \sum_{q \leq b} \sum_{d \leq x/q} f(d)g(q) - \sum_{d \leq a} \sum_{q \leq b} f(d)g(q) \\ &= \sum_{n \leq a} f(n)G\left(\frac{x}{n}\right) + \sum_{n \leq b} g(n)F\left(\frac{x}{n}\right) - F(a)G(b). \end{aligned}$$

□

LEMMA 2.9.4. Sei χ ein reellwertiger Dirichlet-Charakter modulo k , und $A(n) = \sum_{d|n} \chi(d)$. Dann gilt $A(n) \geq 0$ für alle n und $A(n) \geq 1$, falls $n = m^2$ ein Quadrat ist.

BEWEIS. Für Primzahlpotenzen p^α gilt

$$A(p^\alpha) = \sum_{t=0}^{\alpha} \chi(p^t) = 1 + \sum_{t=1}^{\alpha} (\chi(p))^t.$$

Da χ reellwertig ist, kann $\chi(p)$ nur $0, 1, -1$ sein. Für $\chi(p) = 0$ ist $A(p^\alpha) = 1$; für $\chi(p) = 1$ ist $A(p^\alpha) = \alpha + 1$ und für $\chi(p) = -1$ ist

$$A(p^\alpha) = \begin{cases} 1 & \text{falls } \alpha \equiv 0(2), \\ 0 & \text{falls } \alpha \equiv 1(2). \end{cases}$$

Falls α also gerade ist, folgt $A(p^\alpha) \geq 1$ in allen drei Fällen. Sei nun $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Da A multiplikativ ist, folgt $A(n) = A(p_1^{\alpha_1}) \cdots A(p_r^{\alpha_r})$. Jeder Faktor ist größer gleich Null, also auch $A(n) \geq 0$. Ist n ein Quadrat, so sind alle α_i gerade und somit $A(p_i^{\alpha_i}) \geq 1$ für alle i , und deshalb $A(n) \geq 1$. \square

SATZ 2.9.5. Sei $\chi \neq \chi_1$ ein reellwertiger Charakter modulo k und

$$A(n) = \sum_{d|n} \chi(d), \quad B(x) = \sum_{n \leq x} \frac{A(n)}{\sqrt{n}}.$$

Dann gelten:

- (1) $B(x) \rightarrow \infty$ für $x \rightarrow \infty$.
- (2) $B(x) = 2\sqrt{x}L(1, \chi) + O(1)$ für alle $x \geq 1$.
- (3) $L(1, \chi) \neq 0$.

BEWEIS. Zu (3): Wäre $L(1, \chi) = 0$, so wären (1) und (2) unvereinbar.

Zu (1): Mit Lemma 2.9.3 folgt

$$B(x) = \sum_{n \leq x} \frac{A(n)}{\sqrt{n}} \geq \sum_{\substack{n \leq x \\ n=m^2}} \frac{1}{\sqrt{n}} = \sum_{m \leq \sqrt{x}} \frac{1}{m}.$$

Daraus folgt $\lim_{x \rightarrow \infty} B(x) = \sum_{m=1}^{\infty} \frac{1}{m} = \infty$.

Zu (2): Wir wenden Satz 2.9.3 mit $a = b = \sqrt{x}$, also $ab = x$, und $f(n) = \frac{\chi(n)}{\sqrt{n}}$, $g(n) = \frac{1}{\sqrt{n}}$ an:

$$B(x) = \sum_{qd \leq x} \frac{\chi(d)}{\sqrt{qd}} = \sum_{n \leq \sqrt{x}} \frac{\chi(n)}{\sqrt{n}} G\left(\frac{x}{n}\right) + \sum_{n \leq \sqrt{x}} \frac{1}{\sqrt{n}} F\left(\frac{x}{n}\right) - F(\sqrt{x})G(\sqrt{x}).$$

Mit Satz 1.4.4 ist dabei, mit $\sigma = 1/2$ und $A = \zeta(1/2)$:

$$\begin{aligned} G(x) &= \sum_{n \leq x} g(n) = \sum_{n \leq x} \frac{1}{\sqrt{n}} = \frac{x^{1/2}}{1/2} + \zeta\left(\frac{1}{2}\right) + O\left(\frac{1}{\sqrt{x}}\right) \\ &= 2\sqrt{x} + A + O\left(\frac{1}{\sqrt{x}}\right). \end{aligned}$$

Mit (2.6) und $B = \sum_{n=1}^{\infty} \frac{\chi(n)}{\sqrt{n}}$ folgt

$$\begin{aligned} F(x) &= \sum_{n \leq x} \frac{\chi(n)}{\sqrt{n}} = \sum_{n=1}^{\infty} \frac{\chi(n)}{\sqrt{n}} + O\left(\frac{1}{\sqrt{x}}\right) \\ &= B + O\left(\frac{1}{\sqrt{x}}\right). \end{aligned}$$

Zusammen ergibt das $F(\sqrt{x})G(\sqrt{x}) = 2B\sqrt[4]{x} + O(1)$. Setzt man das in die Formel für $B(x)$ oben ein, so erhält man

$$\begin{aligned} B(x) &= \sum_{n \leq \sqrt{x}} \frac{\chi(n)}{\sqrt{n}} \left(2\sqrt{\frac{x}{n}} + A + O\left(\sqrt{\frac{n}{x}}\right)\right) + \sum_{n \leq \sqrt{x}} \frac{1}{\sqrt{n}} \left(B + O\left(\sqrt{\frac{n}{x}}\right)\right) \\ &\quad - 2B\sqrt[4]{x} + O(1). \\ &= 2\sqrt{x} \sum_{n \leq \sqrt{x}} \frac{\chi(n)}{n} + A \sum_{n \leq \sqrt{x}} \frac{\chi(n)}{\sqrt{n}} + O\left(\frac{1}{\sqrt{x}} \sum_{n \leq \sqrt{x}} |\chi(n)|\right) + B \sum_{n \leq \sqrt{x}} \frac{1}{\sqrt{n}} \\ &\quad + O\left(\frac{1}{\sqrt{x}} \sum_{n \leq \sqrt{x}} 1\right) - 2Bx^{1/4} + O(1). \end{aligned}$$

Hierbei ist $\sum_{n \leq \sqrt{x}} \frac{\chi(n)}{\sqrt{n}} = O(1)$ wegen Theorem 2.1.9 und

$$\sum_{n \leq \sqrt{x}} \frac{1}{\sqrt{n}} = 2x^{1/4} + A + O\left(\frac{1}{x^{1/4}}\right)$$

wegen Satz 1.4.4 wie oben, allerdings mit $x^{1/2}$ anstatt mit x . Somit ist in der obigen Gleichung

$$B \sum_{n \leq \sqrt{x}} \frac{1}{\sqrt{n}} - 2Bx^{1/4} = O(1).$$

Zusammen erhält man nun

$$\begin{aligned}
 B(x) &= 2\sqrt{x} \left(\sum_{n \leq x} \frac{\chi(n)}{n} \right) + O(1) \\
 &= 2\sqrt{x} \left(L(1, \chi) + O\left(\frac{1}{x}\right) \right) + O(1) \\
 &= 2\sqrt{x}L(1, \chi) + O(1).
 \end{aligned}$$

□

Nun kommen wir zum Beweis des Theorems von Dirichlet, d.h. von Theorem 2.9.2. Dazu werden Lemma 2.9.6, Lemma 2.9.7, Lemma 2.9.8 und Theorem 2.9.9 gebraucht. Das letzte Theorem besagt, daß $L(1, \chi) \neq 0$ gilt für alle Dirichlet-Charaktere $\chi \neq \chi_1$. Der Beweis dazu ruht noch auf Lemma 2.9.10 und Lemma 2.9.11. Zur Erinnerung, $L(1, \chi)$ und $L'(1, \chi)$ sind ja durch folgende konvergente Reihen gegeben, für $\chi \neq \chi_1$:

$$\begin{aligned}
 L(1, \chi) &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n}, \\
 L'(1, \chi) &= - \sum_{n=1}^{\infty} \frac{\chi(n) \log(n)}{n}.
 \end{aligned}$$

Beweis von Theorem 2.9.2: Sei $k \in \mathbb{N}$ und h relativ prim zu k . Seien $\chi_1, \dots, \chi_{\varphi(k)}$ die Dirichlet-Charaktere modulo k . Der Beweis wird, wie gesagt, durch eine Reihe von Lemmata erbracht, die man dann alle noch beweisen muß. Fangen wir also an mit

LEMMA 2.9.6. Für $x > 1$ gilt

$$\sum_{\substack{p \leq x \\ p \equiv h(k)}} \frac{\log(p)}{p} = \frac{1}{\varphi(k)} \log(x) + \frac{1}{\varphi(k)} \sum_{r=2}^{\varphi(k)} \bar{\chi}_r(h) \sum_{p \leq x} \frac{\chi_r(p) \log(p)}{p} + O(1).$$

Dieses Lemma beweist unser Theorem, sobald wir zeigen können, daß

$$(2.32) \quad \sum_{p \leq x} \frac{\chi_r(p) \log(p)}{p} = O(1), \quad \chi \neq \chi_1.$$

LEMMA 2.9.7. Für $x > 1$ und $\chi \neq \chi_1$ gilt

$$(2.33) \quad \sum_{p \leq x} \frac{\chi_r(p) \log(p)}{p} = -L'(1, \chi) \sum_{n \leq x} \frac{\mu(n) \chi(n)}{n} + O(1).$$

Dieses Lemma wird (2.32) implizieren, sobald wir zeigen können, daß

$$(2.34) \quad \sum_{n \leq x} \frac{\mu(n) \chi(n)}{n} = O(1), \quad \chi \neq \chi_1.$$

LEMMA 2.9.8. Für $x > 1$ und $\chi \neq \chi_1$ gilt

$$(2.35) \quad L(1, \chi) \sum_{n \leq x} \frac{\mu(n) \chi(n)}{n} = O(1).$$

Dieses Lemma wird (2.34) implizieren, und damit (2.32) und unser Theorem, sobald wir zeigen können:

THEOREM 2.9.9. Es gilt $L(1, \chi) \neq 0$ für alle $\chi \neq \chi_1$.

Dieses Theorem ist also der Schlüssel zum Beweis. Nachdem jetzt die Beweisstrategie klar ist, beginnen wir mit den einzelnen Beweisen.

Beweis von Lemma 2.9.6: Wir starten mit Satz 1.5.2 von Mertens, also mit

$$\sum_{p \leq x} \frac{\log(p)}{p} = \log(x) + O(1).$$

Hier wollen wir links diejenigen Terme extrahieren, die zu $p \equiv h(k)$ gehören. Das machen wir mit Theorem 2.1.8, nämlich, für $(n, k) = 1$,

$$\sum_{r=1}^{\varphi(k)} \chi_r(m) \bar{\chi}_r(n) = \begin{cases} \varphi(k) & \text{falls } n \equiv m(k), \\ 0 & \text{sonst.} \end{cases}$$

Wir wählen $m = p, n = h$, bemerken $(n, k) = (h, k) = 1$, multiplizieren obige Gleichung dann mit $\log(p)/p$ und summieren über alle $p \leq x$:

$$\begin{aligned} \varphi(k) \sum_{\substack{p \leq x \\ p \equiv h(k)}} \frac{\log(p)}{p} &= \sum_{p \leq x} \sum_{r=1}^{\varphi(k)} \chi_r(p) \bar{\chi}_r(h) \frac{\log(p)}{p} \\ &= \bar{\chi}_1(h) \sum_{p \leq x} \frac{\chi_1(p) \log(p)}{p} + \sum_{r=2}^{\varphi(k)} \bar{\chi}_r(h) \frac{\chi_r(p) \log(p)}{p} \\ &= \sum_{p \leq x} \frac{\log(p)}{p} + \sum_{r=2}^{\varphi(k)} \bar{\chi}_r(h) \frac{\chi_r(p) \log(p)}{p} + O(1) \\ &= \log(x) + \sum_{r=2}^{\varphi(k)} \bar{\chi}_r(h) \frac{\chi_r(p) \log(p)}{p} + O(1). \end{aligned}$$

Dabei haben wir im letzten Schritt Satz 1.5.2 benutzt. Für die dritte Gleichung haben wir verwendet, daß $\bar{\chi}_1(h) = 1$ und $\chi_1(p) = 1$, falls $(p, k) = 1$ und $\chi_1(p) = 0$ sonst. Dadurch hat man nämlich

$$\begin{aligned} \sum_{p \leq x} \frac{\chi_1(p) \log(p)}{p} &= \sum_{\substack{p \leq x \\ (p, k) = 1}} \frac{\log(p)}{p} = \sum_{p \leq x} \frac{\log(p)}{p} - \sum_{\substack{p \leq x \\ p|k}} \frac{\log(p)}{p} \\ &= \sum_{p \leq x} \frac{\log(p)}{p} + O(1), \end{aligned}$$

denn die Summe über $p \leq x, p | k$ ist beschränkt für alle $x > 1$. Teilt man noch durch $\varphi(k)$, so ist das Lemma bewiesen. \square

Beweis von Lemma 2.9.7: Nach Definition von $\Lambda(n)$ gilt

$$\begin{aligned}
\sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n} &= \sum_{a=1}^{\infty} \sum_{\substack{p \leq x \\ p^a \leq x}} \frac{\chi(p^a) \log(p)}{p^a} \\
&= \sum_{p \leq x} \frac{\chi(p) \log(p)}{p} + \sum_{a=2}^{\infty} \sum_{\substack{p \leq x \\ p^a \leq x}} \frac{\chi(p^a) \log(p)}{p^a} \\
&= \sum_{p \leq x} \frac{\chi(p) \log(p)}{p} + O(1),
\end{aligned}$$

denn die letzte Doppelsumme hat (siehe Bemerkung 1.4.7) die Majorante

$$\sum_p \log(p) \sum_{a=2}^{\infty} p^{-a} = \sum_p \frac{\log(p)}{p(p-1)} < \sum_{n=2}^{\infty} \frac{\log(n)}{n(n-1)} \leq \log(4).$$

Wenn wir jetzt die Relation $\Lambda = \mu * \log$ von Beispiel 1.3.19 verwenden, und dann $n = cd$ schreiben, sowie beachten, daß χ multiplikativ ist, erhalten wir

$$\begin{aligned}
\sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n} &= \sum_{n \leq x} \frac{\chi(n)}{n} \sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right) \\
&= \sum_{d \leq x} \frac{\mu(d)\chi(d)}{d} \sum_{c \leq x/d} \frac{\chi(c) \log(c)}{c}.
\end{aligned}$$

Wegen (2.5) hat man aber

$$\begin{aligned}
\sum_{c \leq x/d} \frac{\chi(c) \log(c)}{c} &= \sum_{c=1}^{\infty} \frac{\chi(c) \log(c)}{c} + O\left(\frac{\log(x/d)}{x/d}\right) \\
&= -L'(1, \chi) + O\left(\frac{\log(x/d)}{x/d}\right),
\end{aligned}$$

und deshalb oben

$$\begin{aligned}
\sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n} &= -L'(1, \chi) \sum_{d \leq x} \frac{\mu(d)\chi(d)}{d} + O\left(\sum_{d \leq x} \frac{1}{d} \frac{\log(x/d)}{x/d}\right) \\
&= -L'(1, \chi) \sum_{d \leq x} \frac{\mu(d)\chi(d)}{d} + O(1).
\end{aligned}$$

Dabei ist der große O -Term einfach ein $O(1)$, weil mit Satz 1.4.5 gilt

$$\begin{aligned} \sum_{d \leq x} \frac{1}{d} \frac{\log(x/d)}{x/d} &= \frac{1}{x} \sum_{d \leq x} (\log(x) - \log(d)) = \frac{1}{x} \left([x] \log(x) - \sum_{d \leq x} \log(d) \right) \\ &= O(1). \end{aligned}$$

Insgesamt folgt also

$$\begin{aligned} \sum_{p \leq x} \frac{\chi(p) \log(p)}{p} &= \sum_{n \leq x} \frac{\chi(n) \Lambda(n)}{n} + O(1) \\ &= -L'(1, \chi) \sum_{d \leq x} \frac{\mu(d) \chi(d)}{d} + O(1). \end{aligned}$$

Beweis von Lemma 2.9.8: Wir wenden die zweite Möbiussche Umkehrformel an (Satz 1.3.22) mit $\alpha(n) = \chi(n)$, $F(x) = x$ und $G(x) = \sum_{n \leq x} \chi(n) \frac{x}{n}$. Dabei können wir $G(x)$ mit (2.4) wie folgt schreiben:

$$G(x) = x \sum_{n \leq x} \frac{\chi(n)}{n} = xL(1, \chi) + O(1).$$

Damit ergibt Satz 1.3.22 also

$$\begin{aligned} x = F(x) &= \sum_{n \leq x} \mu(n) \chi(n) G\left(\frac{x}{n}\right) = \sum_{n \leq x} \mu(n) \chi(n) \left(\frac{x}{n} L(1, \chi) + O(1) \right) \\ &= xL(1, \chi) \sum_{n \leq x} \frac{\mu(n) \chi(n)}{n} + O(x). \end{aligned}$$

Teilt man diese Gleichung durch x , so erhält man die Behauptung.

Beweis von Theorem 2.9.9: Es sei $N(k)$ die Anzahl der Charaktere $\chi \neq \chi_1$ modulo k mit $L(1, \chi) = 0$. Dann gilt auch $L(1, \bar{\chi}) = 0$. Ist χ reellwertig, so folgt die Behauptung aus Satz 2.9.5. Sei also $\bar{\chi} \neq \chi$. Dann ist aber $N(k) \equiv 0(2)$, weil die Charaktere χ mit $L(1, \chi) = 0$ in konjugierten Paaren vorkommen. Das folgende Lemma liefert jetzt den Beweis des Theorems:

LEMMA 2.9.10. Für $x > 1$ gilt

$$(2.36) \quad \sum_{\substack{p \leq x \\ p \equiv 1(k)}} \frac{\log(p)}{p} = \frac{1 - N(k)}{\varphi(k)} \log(x) + O(1).$$

Angenommen, $N(k) \neq 0$. Dann ist $N(k) \geq 2$, da ja $N(k) \in 2\mathbb{N}$. Somit ist $\frac{1 - N(k)}{\varphi(k)} < 0$, so daß die rechte Seite von (2.36) für $x \rightarrow \infty$ gegen $-\infty$ geht. Das ist aber unmöglich, da alle

Terme auf der linken Seite positiv sind. Also ist doch $N(k) = 0$. \square

Beweis von Lemma 2.9.10: Aus Lemma 2.9.6 mit $h = 1$ folgt

$$(2.37) \quad \sum_{\substack{p \leq x \\ p \equiv 1(k)}} \frac{\log(p)}{p} = \frac{1}{\varphi(k)} \log(x) + \frac{1}{\varphi(k)} \sum_{r=2}^{\varphi(k)} \sum_{p \leq x} \frac{\chi_r(p) \log(p)}{p} + O(1).$$

Man beachte, daß wir i.a. $L(1, \chi) \neq 0$ noch nicht wissen. Falls $L(1, \chi_r) \neq 0$, so folgt aus (2.35), daß $\sum_{n \leq x} \frac{\mu(n)\chi(n)}{n} = O(1)$ ist. Dann ist nach (2.33)

$$\begin{aligned} \sum_{p \leq x} \frac{\chi_r(p) \log(p)}{p} &= -L'(1, \chi_r) \sum_{n \leq x} \frac{\mu(n)\chi(n)}{n} + O(1) \\ &= O(1). \end{aligned}$$

Falls aber $L(1, \chi_r) = 0$, so haben wir

$$\sum_{p \leq x} \frac{\chi_r(p) \log(p)}{p} = -\log(x) + O(1),$$

da folgendes Lemma gilt:

LEMMA 2.9.11. *Für jeden Charakter $\chi \neq \chi_1$ mit $L(1, \chi) = 0$ gilt*

$$L'(1, \chi) \sum_{n \leq x} \frac{\mu(n)\chi(n)}{n} = \log(x) + O(1).$$

Zusammen schreibt sich (2.37) also wie folgt:

$$\begin{aligned} \sum_{\substack{p \leq x \\ p \equiv 1(k)}} \frac{\log(p)}{p} &= \frac{1}{\varphi(k)} (-N(k) \log(x) + O(1)) + \frac{1}{\varphi(k)} \log(x) \\ &= \frac{1 - N(k)}{\varphi(k)} \log(x) + O(1). \end{aligned}$$

\square

Beweis von Lemma 2.9.11: Wir wenden Satz 1.3.22 an mit $\alpha(n) = \chi(n)$, $F(x) = x \log(x)$ und

$$\begin{aligned}
G(x) &= \sum_{n \leq x} \chi(n) \frac{x}{n} \log \left(\frac{x}{n} \right) = \sum_{n \leq x} \frac{\chi(n)}{n} x (\log(x) - \log(n)) \\
&= x \log(x) \sum_{n \leq x} \frac{\chi(n)}{n} - x \sum_{n \leq x} \frac{\chi(n) \log(n)}{n} \\
&= x \log(x) (L(1, \chi) + O(x^{-1})) + x \left(L'(1, \chi) + O \left(\frac{\log(x)}{x} \right) \right) \\
&= xL'(1, \chi) + O(\log(x)).
\end{aligned}$$

Dabei haben wir Korollar 2.1.10 verwendet. Satz 1.3.22 ergibt damit

$$\begin{aligned}
x \log(x) &= \sum_{n \leq x} \mu(n) \chi(n) \left(\frac{x}{n} L'(1, \chi) + O \left(\log \left(\frac{x}{n} \right) \right) \right) \\
&= xL'(1, \chi) \sum_{n \leq x} \frac{\mu(n) \chi(n)}{n} + O \left(\sum_{n \leq x} (\log(x) - \log(n)) \right) \\
&= xL'(1, \chi) \sum_{n \leq x} \frac{\mu(n) \chi(n)}{n} + O(x).
\end{aligned}$$

Nach Division durch x erhalten wir die Behauptung. Damit ist auch Dirichlets Theorem vollständig bewiesen. \square

Analog zur Funktion $\pi(x)$ können wir auch folgende Zählfunktion betrachten.

DEFINITION 2.9.12. Sei $k > 0$ und $(h, k) = 1$. Für $x \geq 1$ definiere

$$\pi_{h,k}(x) = \sum_{\substack{p \leq x \\ p \equiv h(k)}} 1.$$

Dirichlets Theorem zeigt, daß $\pi_{h,k}(x) \rightarrow \infty$ für $x \rightarrow \infty$. Der Hauptterm in (2.31), nämlich $\log(x)/\varphi(k)$, hängt dabei gar nicht von h ab. Die Primzahlen scheinen also gleichverteilt zu sein unter den $\varphi(k)$ Restklassen modulo k . In der Tat, es gilt der sogenannte Primzahlsatz für arithmetische Progressionen:

THEOREM 2.9.13 (PNT2). Sei $k > 0$ und $(h, k) = 1$. Dann gilt

$$\pi_{h,k}(x) \sim \frac{1}{\varphi(k)} \frac{x}{\log(x)}, \quad x \rightarrow \infty.$$

BEMERKUNG 2.9.14. Man kann aus Theorem 2.9.9 auch folgendes Resultat ableiten, vergleiche Bemerkung 1.1.14: Es existiert eine Konstante $C = C(h, k)$ so daß für alle $x \geq 2$ gilt:

$$\sum_{\substack{p \leq x \\ p \equiv h(k)}} \frac{1}{p} = \frac{1}{\varphi(k)} \log(\log(x)) + C + O\left(\frac{1}{x}\right).$$

Abschließend wollen wir noch erwähnen, daß der *Dichtesatz von Chebotarev* eine Verallgemeinerung von Dirichlets Theorem ist:

THEOREM 2.9.15. *Sei K ein Zahlkörper und L/K eine Galois-Erweiterung mit $G = \text{Gal}(L/K)$. Für $\sigma \in G$ sei C_σ die Konjugationsklasse von σ . Sei S die Menge der Primideale \mathfrak{p} von K , so daß für jedes Primideal \mathfrak{P} von L , das über \mathfrak{p} liegt, das Frobeniuselement von \mathfrak{P} in C_σ liegt. Dann hat S Dirichletdichte $\frac{|C_\sigma|}{|G|}$.*

Dirichlets Theorem erhält man mit folgender Spezialisierung. Sei $K = \mathbb{Q}$ und $L = \mathbb{Q}(\zeta_k)$ mit einer primitiven k -ten EW ζ_k . Dann ist L eine abelsche Erweiterung von \mathbb{Q} mit $G = (\mathbb{Z}/k\mathbb{Z})^*$, so daß $C_\sigma = \{\sigma\}$ für alle $\sigma \in G$. Das Frobeniuselement von \mathfrak{P} ist das Artin-Symbol $\left(\frac{\mathbb{Q}(\zeta_k)/\mathbb{Q}}{p}\right) = \bar{p} \in (\mathbb{Z}/k\mathbb{Z})^*$, für alle \mathfrak{P} über Primzahlen p mit $p \nmid k$. Die Konjugationsklassen modulo k von Primzahlen, die nicht k teilen stehen daher in bijektiver Korrespondenz zu den Elementen von G . Also ist die Menge S oben von der Gestalt

$$S_h = \{p \in \mathbb{P} \mid p \equiv h(k)\}.$$

Wegen $|C_\sigma| = 1$ und $|G| = \varphi(k)$ hat die Menge S_h die Dirichletdichte $\frac{1}{\varphi(k)}$ für jedes $h \in (\mathbb{Z}/k\mathbb{Z})^*$. Das ist genau Dirichlets Theorem.

CHAPTER 3

Dirichlet-Reihen, Riemannsches ζ -Funktion und L -Reihen

Die analytischen Eigenschaften von Dirichlet-Reihen, insbesondere die der Riemannsches ζ -Funktion, spielen eine wichtige Rolle in der Zahlentheorie. Wir beginnen mit allgemeinen Eigenschaften von Dirichlet-Reihen.

3.1. Dirichlet-Reihen

DEFINITION 3.1.1. Eine *Dirichlet-Reihe* ist eine Reihe der Gestalt

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

wobei f eine arithmetische Funktion ist und $s = \sigma + it \in \mathbb{C}$.

Für $f(n) = 1$ ist $F(s) = \zeta(s)$, und für $f(n) = \chi(n)$ ist $F(s) = L(s, \chi)$. Die Menge der Punkte $s = \sigma + it$ mit $\sigma > a$ heißt *Halbebene* in \mathbb{C} . Für $\sigma \geq a$ gilt $|n^s| = n^\sigma \geq n^a$, und deshalb

$$\left| \frac{f(n)}{n^s} \right| \leq \frac{|f(n)|}{n^a}.$$

Konvergiert also eine Dirichlet-Reihe $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ absolut für ein $s = a + ib$, so konvergiert sie nach dem Majorantenkriterium auch absolut für alle s mit $\sigma \geq a$.

SATZ 3.1.2. *Angenommen, die Reihe $\sum_{n=1}^{\infty} |f(n)n^{-s}|$ konvergiert nicht für alle s , oder divergiert nicht für alle s . Dann gibt es eine reelle Zahl σ_a , die Abszisse der absoluten Konvergenz, so daß die Reihe $\sum_{n=1}^{\infty} f(n)n^{-s}$ für $\sigma > \sigma_a$ absolut konvergiert, und für $\sigma < \sigma_a$ aber nicht.*

BEWEIS. Sei D die Menge der $\sigma \in \mathbb{R}$, für die $\sum_{n=1}^{\infty} |f(n)n^{-s}|$ divergiert. Nach Voraussetzung ist $D \neq \emptyset$, und D ist nach oben beschränkt. Also hat D eine kleinste obere Schranke $\sigma_a := \sup(D)$. Für $\sigma < \sigma_a$ folgt $\sigma \in D$, sonst wäre σ eine kleinere obere Schranke für D als $\sup(D)$, was unmöglich ist. Für $\sigma > \sigma_a$ folgt $\sigma \notin D$, da σ_a eine obere Schranke für D ist. Wir setzen noch $\sigma_a = -\infty$, falls $\sum_{n=1}^{\infty} |f(n)n^{-s}|$ überall konvergiert, und $\sigma_a = \infty$, falls $\sum_{n=1}^{\infty} |f(n)n^{-s}|$ nirgends konvergiert. \square

BEISPIEL 3.1.3. *Für $\zeta(s)$ und $L(s, \chi)$ ist $\sigma_a = 1$. Für $\sum_{n=1}^{\infty} n^n n^{-s}$ ist $\sigma_a = \infty$, und für $\sum_{n=1}^{\infty} n^{-n} n^{-s}$ ist $\sigma_a = -\infty$.*

$\zeta(s)$ konvergiert absolut für $\sigma > 1$ und divergiert bei $s = 1$. Also ist $\sigma_a = 1$. Ist f beschränkt, also $|f(n)| \leq C$, so konvergiert $\sum_{n=1}^{\infty} f(n)n^{-s}$ absolut für $\sigma > 1$. Das trifft insbesondere für $L(s, \chi)$ zu, da χ beschränkt ist. Die dritte Reihe konvergiert nirgends, die vierte überall in \mathbb{C} .

SATZ 3.1.4. Sei $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$. Dann gilt $\lim_{\sigma \rightarrow \infty} F(\sigma + it) = f(1)$ gleichmäßig für $-\infty < t < \infty$.

BEWEIS. Wir schreiben $F(s) = f(1) + \sum_{n=2}^{\infty} f(n)n^{-s}$. Wir müssen zeigen, daß die Reihe gegen Null konvergiert für $\sigma \rightarrow \infty$. Wähle ein $c > \sigma_a$. Für $\sigma \geq c$ haben wir

$$\begin{aligned} \left| \sum_{n=2}^{\infty} f(n)n^{-s} \right| &\leq \sum_{n=2}^{\infty} |f(n)|n^{-\sigma} = \sum_{n=2}^{\infty} |f(n)|n^{-c}n^{-(\sigma-c)} \\ &\leq 2^{-(\sigma-c)} \sum_{n=2}^{\infty} |f(n)|n^{-c} = 2^{-\sigma} A, \end{aligned}$$

wobei A von σ und t unabhängig ist. Wegen $\lim_{\sigma \rightarrow \infty} 2^{-\sigma} A = 0$ folgt die Behauptung. \square

KOROLLAR 3.1.5. Es gilt $\lim_{\sigma \rightarrow \infty} \zeta(\sigma + it) = \lim_{\sigma \rightarrow \infty} L(\sigma + it, \chi) = 1$.

Das folgende Eindeutigkeitstheorem ist von Nutzen.

THEOREM 3.1.6 (Eindeutigkeit). Seien $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ und $G(s) = \sum_{n=1}^{\infty} g(n)n^{-s}$ zwei Dirichlet-Reihen, die beide für $\sigma > \sigma_a$ absolut konvergieren. Sei (s_k) eine unendliche Folge komplexer Zahlen mit $\lim_{k \rightarrow \infty} \sigma_k = \infty$. Gilt $F(s) = G(s)$ für alle $s = s_k$, so folgt $f(n) = g(n)$ für alle $n \in \mathbb{N}$.

Man beachte $s_k = \sigma_k + it_k$. Wir verzichten auf den Beweis, der aber nicht schwer ist (siehe [1]). Als Konsequenz erhalten wir

SATZ 3.1.7. Sei $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ eine Dirichlet-Reihe mit $F(s) \neq 0$ für ein s mit $\sigma > \sigma_a$. Dann gibt es eine Halbebene $\sigma > c \geq \sigma_a$, in der $F(s)$ niemals verschwindet.

BEWEIS. Angenommen, es gibt keine solche Halbebene. Dann gibt es für jedes $k \in \mathbb{N}$ einen Punkt s_k mit $\sigma_k = \operatorname{Re}(s_k) > k$ mit $F(s_k) = 0$. Wegen $\lim_{k \rightarrow \infty} \sigma_k = \infty$ folgt also $f(n) = 0$ mit dem Eindeutigkeitsatz. Dann wäre $F(s) = 0$ überall, Widerspruch. \square

SATZ 3.1.8. Es seien $F(s)$ und $G(s)$ zwei Funktionen, die durch die Dirichlet-Reihen

$$\begin{aligned} F(s) &= \sum_{n=1}^{\infty} f(n)n^{-s}, \quad \sigma > a, \\ G(s) &= \sum_{n=1}^{\infty} g(n)n^{-s}, \quad \sigma > b, \end{aligned}$$

gegeben sind. Dann gilt in der Halbebene, in der beide Reihen absolut konvergieren

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

wobei $(f * g)(n) = \sum_{d|n} f(d)g(n/d)$ die Dirichlet-Konvolution von f und g ist.

BEWEIS. Wir haben

$$\begin{aligned} F(s)G(s) &= \sum_{n=1}^{\infty} f(n)n^{-s} \sum_{m=1}^{\infty} g(m)m^{-s} = \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} f(n)g(m)(nm)^{-s} \\ &= \sum_{k=1}^{\infty} \left(\sum_{mn=k} f(n)g(m) \right) k^{-s} = \sum_{k=1}^{\infty} (f * g)(k)k^{-s}. \end{aligned}$$

Hierbei sei s so gewählt, daß beide Reihen absolut konvergieren. Wir dürfen also beliebig umsortieren. Man sammelt dann die Terme, für die $mn = k$ konstant ist, und erhält das Resultat. \square

BEISPIEL 3.1.9. *Es gilt $\zeta(s) \neq 0$ für $\sigma > 1$ und*

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

Man wählt $F(s) = \zeta(s)$ und $G(s) = \sum_{n=1}^{\infty} \mu(n)n^{-s}$ in Satz 3.1.8. Diese Reihen konvergieren absolut für $\sigma > 1$. Man erhält $(f * g)(n) = (\varepsilon * \mu)(n) = I(n)$, so daß

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

BEISPIEL 3.1.10. *Sei χ ein Dirichlet-Charakter modulo k . Dann gilt für $\sigma > 1$*

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

Konvergiert $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ absolut für $\sigma > \sigma_a$, und ist f streng multiplikativ, so hat man $f^{-1}(n) = \mu(n)f(n)$. Wegen $|f^{-1}(n)| \leq |f(n)|$ konvergiert auch die Reihe $\sum_{n=1}^{\infty} \mu(n)f(n)n^{-s}$ absolut für $\sigma > \sigma_a$, und es gilt

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

Für $f(n) = \chi(n)$ folgt obige Behauptung.

BEISPIEL 3.1.11. *Für $\sigma > 2$ gilt*

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

Dazu nimmt man $f(n) = 1$, $g(n) = \varphi(n)$ und $(f * g)(n) = \sum_{d|n} \varphi(d) = n$. Wegen $\varphi(n) \leq n$ konvergiert die Reihe $\sum_{n=1}^{\infty} \varphi(n)n^{-s}$ absolut für $\sigma > 2$. Satz 3.1.8 liefert also

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

Weitere Identitäten dieser Art, auch die aus Bemerkung 1.2.14, lassen sich ebenso zeigen:

$$\sum_{n=1}^{\infty} \mu^2(n)n^{-s} = \frac{\zeta(s)}{\zeta(2s)}, \quad \sigma > 1$$

$$\sum_{n=1}^{\infty} 2^{\omega(n)}n^{-s} = \frac{\zeta^2(s)}{\zeta(2s)}, \quad \sigma > 1$$

$$\sum_{n=1}^{\infty} \tau(n^2)n^{-s} = \frac{\zeta^3(s)}{\zeta(2s)}, \quad \sigma > 1$$

$$\sum_{n=1}^{\infty} \tau^2(n)n^{-s} = \frac{\zeta^4(s)}{\zeta(2s)}, \quad \sigma > 1.$$

3.2. Euler-Produkte

Durch die Eulerprodukt-Darstellung erhält man den Bezug zwischen Dirichlet-Reihen und den Primzahlen. Das ist natürlich sehr wichtig in der Zahlentheorie.

SATZ 3.2.1. *Sei f eine multiplikative arithmetische Funktion, so daß die Reihe $\sum_{n=1}^{\infty} f(n)$ absolut konvergent ist. Dann gilt*

$$\sum_{n=1}^{\infty} f(n) = \prod_{p \in \mathbb{P}} \left(\sum_{k=0}^{\infty} f(p^k) \right),$$

wobei das unendliche Produkt absolut konvergent ist. Ist f streng multiplikativ, so hat man

$$\sum_{n=1}^{\infty} f(n) = \prod_{p \in \mathbb{P}} \frac{1}{1 - f(p)}.$$

BEWEIS. Man betrachte zuerst das endliche Produkt

$$P(x) = \prod_{p \leq x} (1 + f(p) + f(p^2) + \dots).$$

Das ist ein Produkt von endlich vielen, absolut konvergenten Reihen, die wir multiplizieren und die Terme umordnen können, ohne die Summe zu ändern. Ein typischer Term von $P(x)$ hat die Gestalt $f(p_1^{\alpha_1}) \cdots f(p_r^{\alpha_r}) = f(p_1^{\alpha_1} \cdots p_r^{\alpha_r})$. Nach dem Fundamentalsatz der Arithmetik hat man $P(x) = \sum_{n \in A} f(n)$, wobei A die Menge der $n \in \mathbb{N}$ ist, für die gilt: alle Primteiler $p \mid n$ erfüllen $p \leq x$. Ist B die Menge der n , die mindestens einen Primfaktor $p > x$ hat, so folgt

$$\left| \sum_{n=1}^{\infty} f(n) - P(x) \right| \leq \sum_{n \in B} |f(n)| \leq \sum_{n > x} |f(n)|.$$

Da die Reihe $\sum_{n=1}^{\infty} |f(n)|$ konvergent ist, geht die rechte Seite für $x \rightarrow \infty$ gegen Null. Also ist

$$\lim_{x \rightarrow \infty} \left(P(x) - \sum_{n=1}^{\infty} f(n) \right) = 0.$$

Ist f streng multiplikativ, so ist $f(p^n) = f(p)^n$ und deshalb $\sum_{k=0}^{\infty} (f(p))^k = (1 - f(p))^{-1}$. Das zeigt die Behauptung. Wir zeigen noch, warum das Produkt absolut konvergiert. Ein Produkt $\prod_{n=1}^{\infty} (1 + a_n)$ konvergiert ja absolut, wenn die Reihe $\sum_{n=1}^{\infty} a_n$ absolut konvergiert. Die Reihe $\sum_p |f(p) + f(p^2) + \dots|$ konvergiert aber absolut wegen

$$\sum_{p \leq x} |f(p) + f(p^2) + \dots| \leq \sum_{p \leq x} (|f(p)| + |f(p^2)| + \dots) \leq \sum_{n=2}^{\infty} |f(n)|.$$

□

Aus diesem Satz erhält man mit $g(n) = f(n)n^{-s}$ sofort

SATZ 3.2.2. *Sei f eine multiplikative arithmetische Funktion, so daß die Dirichlet-Reihe $\sum_{n=1}^{\infty} f(n)n^{-s}$ absolut konvergent ist für $\sigma > \sigma_a$. Dann gilt*

$$\sum_{n=1}^{\infty} f(n)n^{-s} = \prod_{p \in \mathbb{P}} \left(\sum_{k=0}^{\infty} f(p^k)p^{-ks} \right), \quad \sigma > \sigma_a.$$

Ist f streng multiplikativ, so hat man

$$\sum_{n=1}^{\infty} f(n)n^{-s} = \prod_{p \in \mathbb{P}} \frac{1}{1 - f(p)p^{-s}}, \quad \sigma > \sigma_a.$$

Für unsere bekannten arithmetischen Funktionen erhält man damit folgende Euler-Produkte:

$$\begin{aligned} \sum_{n=1}^{\infty} n^{-s} &= \zeta(s) = \prod_p \frac{1}{1 - p^{-s}}, \quad \sigma > 1, \\ \sum_{n=1}^{\infty} \mu(n)n^{-s} &= \frac{1}{\zeta(s)} = \prod_p (1 - p^{-s}), \quad \sigma > 1, \\ \sum_{n=1}^{\infty} \varphi(n)n^{-s} &= \frac{\zeta(s-1)}{\zeta(s)} = \prod_p \frac{1 - p^{-s}}{1 - p^{1-s}}, \quad \sigma > 2, \\ \sum_{n=1}^{\infty} \lambda(n)n^{-s} &= \frac{\zeta(2s)}{\zeta(s)} = \prod_p \frac{1}{1 + p^{-s}}, \quad \sigma > 1, \\ \sum_{n=1}^{\infty} \sigma_{\alpha}(n)n^{-s} &= \zeta(s)\zeta(s-\alpha) = \prod_p \frac{1}{(1 - p^{-s})(1 - p^{\alpha-s})}, \quad \sigma > b, \\ \sum_{n=1}^{\infty} \tau(n)n^{-s} &= \zeta(s)^2 = \prod_p (1 - p^{-s})^{-2}, \quad \sigma > 1, \\ \sum_{n=1}^{\infty} \chi(n)n^{-s} &= L(s, \chi) = \prod_p \frac{1}{1 - \chi(p)p^{-s}}, \quad \sigma > 1, \\ \sum_{n=1}^{\infty} \mu^2(n)n^{-s} &= \frac{\zeta(s)}{\zeta(2s)} = \prod_p (1 + p^{-s}), \quad \sigma > 1, \end{aligned}$$

wobei $b = \max\{1, 1 + \operatorname{Re}(\alpha)\}$. Hat man die Euler-Produkte von $F(s)$ ausgerechnet, so kann man damit wiederum die Darstellung durch Zetafunktionen ableiten. Das hatten wir ja vorher ohne Euler-Produkte mit Satz 3.1.8 getan.

3.3. Analytische Fortsetzung von $\zeta(s)$

Die Riemannsche ζ -Funktion ist zunächst nur für $\sigma > 1$ definiert, und dort eine holomorphe Funktion. Wir hatten in Satz 1.4.4 schon gesehen, wie wir $\zeta(s)$ auf die Halbebene $\sigma > 0$ analytisch fortsetzen können. Dazu benutzt man die ESF, um für $\sigma > 1$ zu zeigen:

$$\zeta(s) = 1 - \frac{1}{1-s} - s \int_1^\infty \frac{t - [t]}{t^{s+1}} dt.$$

Man kann zeigen, daß die rechte Seite absolut und gleichmäßig konvergiert für $\operatorname{Re}(s) \geq \sigma > 0$. Mit dem Theorem von Weierstrass ist dieses Integral also eine holomorphe Funktion von s in der Halbebene $\sigma > 0$. Es stellt damit eine explizite analytische Fortsetzung von $\zeta(s)$ auf die Halbebene $\sigma > 0$ dar.

Man kann diese Idee so verallgemeinern, daß man eine Fortsetzung auf ganz \mathbb{C} erhält. Wir wollen hier aber einen anderen Beweis für die Fortsetzbarkeit präsentieren:

THEOREM 3.3.1. *Die Funktion $\zeta(s)$ kann analytisch fortgesetzt werden zu einer meromorphen Funktion auf ganz \mathbb{C} , mit einer einzigen Singularität, die ein einfacher Pol bei $s = 1$ mit Residuum 1 ist.*

BEWEIS. Die Gamma-Funktion hat die Integraldarstellung

$$\Gamma(s) = \int_0^\infty t^{s-1} e^{-t} dt, \quad \sigma > 0.$$

Sie kann nach ganz \mathbb{C} meromorph fortgesetzt werden mit einfachen Polen bei $s = 0, -1, -2, -3, \dots$ mit Residuum $\frac{(-1)^n}{n!}$ bei $s = -n$. Die Gammafunktion erfüllt die Funktionalgleichungen

$$\begin{aligned} \Gamma(s+1) &= s\Gamma(s) \\ \Gamma(s)\Gamma(1-s) &= \frac{\pi}{\sin(\pi s)}. \end{aligned}$$

Wir starten nun mit der Formel

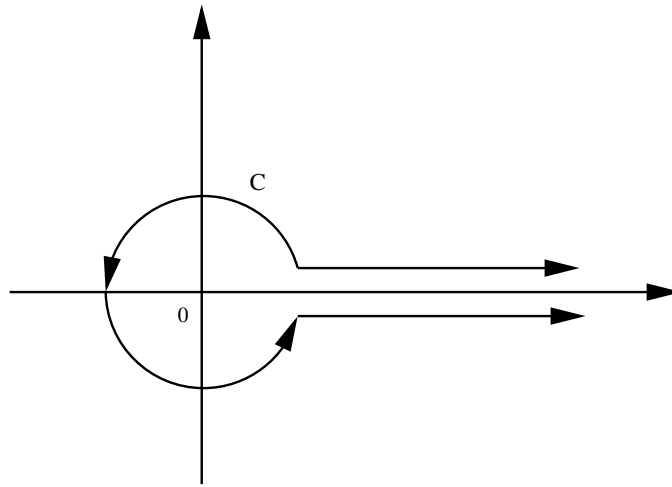
$$\Gamma(s)n^{-s} = \int_0^\infty t^{s-1} e^{-nt} dt, \quad \sigma > 0.$$

Summiert man über $n \geq 1$, dann gilt für $\sigma > 1$

$$\Gamma(s)\zeta(s) = \sum_{n=1}^{\infty} \int_0^\infty t^{s-1} e^{-nt} dt = \int_0^\infty \frac{t^{s-1}}{e^t - 1} dt.$$

Wir erhalten wie folgt eine analytische Fortsetzung dieses Integrals: wir ersetzen die Halbgerade $[0, \infty]$ der Integration durch den *Hankelweg* $C = C_\rho$ in \mathbb{C} , wobei $0 < \rho < 2\pi$ ein reeller

Parameter ist:



Der Weg C_ρ besteht aus drei Teilen: der Menge der Punkte mit Argument $0+$ auf der reellen Halbgeraden $[\rho, \infty]$, dem Kreis $|z| = \rho$, und der Menge der Punkte mit Argument $2\pi-$ auf der Halbgeraden $[\rho, \infty]$ in umgekehrter Orientierung. Der erste und dritte Teil sind die obere und untere Kante eines Schlitzes entlang der positiven Halbgeraden. Das Bild ist etwas irreführend. Dort hat der Weg einen Abstand ε von der reellen Achse. Man muß sich aber den Limes solcher Wege für $\varepsilon \rightarrow 0$ vorstellen. Da die Funktion $z \mapsto z^{s-1}(e^z - 1)^{-1}$ holomorph im horizontalen Streifen $|\operatorname{Im}(z)| < 2\pi$ ohne die Halbgerade $[0, \infty]$ ist, ist das Integral

$$I(s) := \int_{C_\rho} z^{s-1}(e^z - 1)^{-1} dz$$

unabhängig von ρ in $(0, 2\pi)$. Es ist absolut konvergent für alle $s \in \mathbb{C}$ und gleichmäßig konvergent auf jedem Kompaktum. Also definiert $I(s)$ eine ganze Funktion. Es gilt

$$(3.1) \quad I(s) = \int_{|z|=\rho} z^{s-1}(e^z - 1)^{-1} dz + (e^{2\pi is} - 1) \int_\rho^\infty t^{s-1}(e^t - 1)^{-1} dt.$$

Nun läßt man ρ gegen Null gehen. Für $|z| = \rho \leq \pi$ ist $|z^{s-1}(e^z - 1)^{-1}| = O(\rho^{\sigma-2})$. Man erhält also die Formel

$$I(s) = (e^{2\pi is} - 1)\Gamma(s)\zeta(s), \quad \sigma > 1.$$

Also folgt mit $\Gamma(s)\Gamma(1-s) = \pi/\sin(\pi s)$

$$(3.2) \quad \zeta(s) = \frac{1}{2\pi i} e^{-i\pi s} \Gamma(1-s) I(s).$$

Diese Formel, ursprünglich nur für $\sigma > 1$ gültig, liefert nun eine explizite analytische Fortsetzung von $\zeta(s)$ auf $\mathbb{C} \setminus 1$. Für $\sigma \leq 0$ ist der Faktor $\Gamma(1-s)$ holomorph. Also hat $\zeta(s)$ keine weitere Singularität außer der bei $s = 1$. \square

DEFINITION 3.3.2. Sei $0 < a \leq 1$. Für $\sigma > 1$ ist die *Hurwitzsche Zetafunktion* $\zeta(s, a)$ definiert durch die Reihe

$$\zeta(s, a) = \sum_{n=0}^{\infty} \frac{1}{(n+a)^s}.$$

Es ist $\zeta(s, 1) = \zeta(s)$ und man kann auch $L(s, \chi)$ mit Hilfe der Hurwitz ζ -Funktion ausdrücken. Ganz analog zu oben kann man zeigen, daß $\zeta(s, a)$ eine analytische Fortsetzung auf $\mathbb{C} \setminus 1$ hat, mit einem einfachen Pol bei $s = 1$ mit Residuum 1. Daran sieht man dann auch, daß man $L(s, \chi)$ für $\chi \neq \chi_1$ auf ganz \mathbb{C} analytisch fortsetzen kann. Dagegen kann man $L(s, \chi_1)$ analytisch auf $\mathbb{C} \setminus 1$ fortsetzen, mit einem einfachen Pol bei $s = 1$ mit Residuum $\varphi(k)/k$. Wir notieren noch eine Folgerung aus (3.1). Sei B_n die n -te Bernoulli-Zahl. Man kann sie definieren durch die folgende Laurent-Entwicklung

$$\frac{1}{e^z - 1} = \sum_{m=0}^{\infty} \frac{1}{m!} B_m z^{m-1}.$$

Es ist leicht zu sehen, daß $B_{2m+1} = 0$ für $m \geq 1$ und $B_1 = -1/2$. Hier sind einige weitere Werte:

m	2	4	6	8	10	12	14	16	18	20
B_m	$\frac{1}{6}$	$-\frac{1}{30}$	$\frac{1}{42}$	$-\frac{1}{30}$	$\frac{5}{66}$	$-\frac{691}{2730}$	$\frac{7}{6}$	$-\frac{3617}{510}$	$\frac{43867}{798}$	$-\frac{174611}{330}$

SATZ 3.3.3. Für alle $n \geq 0$ gilt

$$\zeta(-n) = (-1)^n \frac{B_{n+1}}{n+1} = -\frac{B_{n+1}}{n+1}.$$

Inbesondere ist $\zeta(-2n) = 0$ für alle $n \geq 1$.

BEWEIS. Mit (3.1) folgt

$$I(-n) = \int_{|z|=\rho} z^{-n-1} (e^z - 1)^{-1} dz = 2\pi i \frac{B_{n+1}}{(n+1)!}.$$

Setzt man das in (3.2) mit $s = -n$ ein, so folgt die Behauptung wegen $\Gamma(n+1) = n!$ und $\cos(\pi n) = (-1)^n$. Man beachte, daß $B_{n+1} = 0$ ist für gerades n , und $(-1)^n = -1$ für ungerades n . Deshalb kann man $(-1)^n$ oben durch -1 ersetzen. \square

3.4. Die Funktionalgleichung für $\zeta(s)$ und $L(s, \chi)$

Die sogenannte Verdopplungsformel für die Gammafunktion ist gegeben durch

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

Um die Funktionalgleichung für $\zeta(s)$ in ästhetisch ansprechender Form schreiben zu können, führen wir die Notation $\Phi(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s)$ ein. Mit der Verdopplungsformel sieht man, daß die Funktionalgleichung $\Phi(s) = \Phi(1-s)$ äquivalent ist zu:

THEOREM 3.4.1. *Für jedes $s \neq 1$ haben wir*

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

oder $\Phi(s) = \Phi(1-s)$ mit $s \neq 0, 1$.

BEWEIS. Für $k \geq 1$ sei H_k der Hankelweg mit Parameter $\rho_k = (2k+1)\pi$. Dann ist $|e^z - 1|^{-1}$ beschränkt für z auf H_k , und wir haben

$$(3.3) \quad \left| \int_{H_k} z^{s-1} (e^z - 1)^{-1} dz \right| = O(k^\sigma).$$

Sei ρ gegeben mit $0 < \rho < 2\pi$. Der Weg $C_\rho - H_k$ umrundet die Pole $z = 2n\pi i$ für $n = \pm 1, \pm 2, \dots, \pm k$ gegen den Urzeigersinn. Der Residuensatz liefert dann

$$\begin{aligned} I(s) &= \int_{C_\rho} z^{s-1} (e^z - 1)^{-1} dz \\ &= \int_{H_k} z^{s-1} (e^z - 1)^{-1} dz - 2\pi i \sum_{1 \leq |n| \leq k} (2n\pi i)^{s-1} \\ &= \int_{H_k} z^{s-1} (e^z - 1)^{-1} dz - (2\pi i)^s (1 - e^{i\pi s}) \sum_{1 \leq n \leq k} n^{s-1}. \end{aligned}$$

Mit (3.3) erhalten wir für $k \rightarrow \infty$ und für jedes s in der Halbebene $\sigma < 0$

$$I(s) = (2\pi i)^s (e^{i\pi s} - 1) \zeta(1-s).$$

Setzt man das in (3.2) ein, so erhält man die Funktionalgleichung für $\sigma < 0$. Durch analytische Fortsetzung bleibt sie dann auch für alle s gültig. \square

KOROLLAR 3.4.2. Für $n \geq 1$ gilt

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

BEWEIS. Satz 3.3.3 liefert

$$\zeta(1 - 2n) = -\frac{B_{2n}}{2n}.$$

Die Funktionalgleichung für $s = 1 - 2n$ ist äquivalent zu

$$\zeta(2n) = 2^{2n-1} \pi^{2n} (\sin(\pi/2 - \pi n))^{-1} \zeta(1 - 2n).$$

Setzt man $\zeta(1 - 2n)$ darin ein und beachtet noch $\sin(\pi/2 - \pi n) = \cos(-\pi n) = (-1)^n$, so folgt die Behauptung. \square

BEISPIEL 3.4.3. Für $n = 1, \dots, 7$ erhält man

$$\begin{aligned} \zeta(2) &= \frac{\pi^2}{6}, & \zeta(4) &= \frac{\pi^4}{90}, & \zeta(6) &= \frac{\pi^6}{945}, & \zeta(8) &= \frac{\pi^8}{9450} \\ \zeta(10) &= \frac{\pi^{10}}{93555}, & \zeta(12) &= \frac{691\pi^{12}}{638512875}, & \zeta(14) &= \frac{2\pi^{14}}{18243225}. \end{aligned}$$

Die Brüche werden sehr schnell unangenehm groß. So ist $\zeta(50)$ schon recht unhandlich:

$$\zeta(50) = \frac{39604576419286371856998202\pi^{50}}{285258771457546764463363635252374414183254365234375}.$$

Man sollte hierbei erwähnen, daß man über die Werte $\zeta(2n + 1)$ sehr wenig weiß. Apéry konnte 1978 zeigen, daß $\zeta(3)$ irrational ist. Er fand auch folgende interessante Formel für $\zeta(3)$:

$$\zeta(3) = \frac{5}{2} \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^3 \binom{2n}{n}}.$$

Man vermutet sogar, daß die Zahlen

$$\zeta(3), \zeta(5), \zeta(7), \zeta(9), \dots$$

alle algebraisch unabhängig sind. Bisher allerdings ist man schon froh, wenn man etwas über die \mathbb{Q} -Dimension des Vektorraumes sagen kann, der von Werten $\zeta(2n + 1)$ aufgespannt wird.

W. Zudilin zeigte, daß mindestens eine der Zahlen $\zeta(5), \zeta(7), \zeta(9), \zeta(11)$ irrational ist.

Für reelles a und $\sigma > 1$ sei

$$F(a, s) = \sum_{n=1}^{\infty} \frac{e^{2\pi i n a}}{n^s}.$$

Diese Funktion ist eine periodische Funktion von a mit Periode 1 mit $F(1, s) = \zeta(s)$. Die Reihe konvergiert absolut für $\sigma > 1$. Wir erwähnen die Hurwitzsche Formel (für einen Beweis siehe [1]):

SATZ 3.4.4. *Für $0 < a \leq 1$ und $\sigma > 1$ gilt*

$$\zeta(1-s, a) = \frac{\Gamma(s)}{(2\pi)^s} (e^{-\pi i s/2} F(a, s) + e^{\pi i s/2} F(-a, s)).$$

Für $a = 1$ erhält man die Funktionalgleichung in der Gestalt

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

zurück. Mit der Hurwitzschen Formel kann man auch eine Funktionalgleichung für Dirichletsche L -Funktionen ableiten. Dabei genügt es, primitive Dirichlet-Charaktere zu betrachten. Das Ergebnis ist:

SATZ 3.4.5. *Sei χ ein primitiver Dirichlet-Charakter modulo k . Dann gilt für alle s*

$$L(1-s, \chi) = \frac{k^{s-1} \Gamma(s)}{(2\pi)^s} (e^{-\pi i s/2} + \chi(-1) e^{\pi i s/2}) G(1, \chi) L(s, \bar{\chi}).$$

3.5. Die Nullstellen von $\zeta(s)$

Die Konvergenz des Euler-Produktes

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

garantiert, daß $\zeta(s)$ nicht verschwindet für $\sigma > 1$. Wir wollen hier zeigen, daß $\zeta(s)$ auch nicht auf der Geraden $\sigma = 1$ verschwindet. Dieses Resultat wird in vielen Beweisen des PNT verwendet (siehe zum Beispiel [17]).

SATZ 3.5.1. *Sei $F(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ eine Dirichlet-Reihe mit nicht-negativen Koeffizienten und mit Konvergenzabszisse σ_c . Dann gilt für alle $\sigma > \sigma_c$*

$$3F(\sigma) + 4\operatorname{Re}F(\sigma + it) + \operatorname{Re}F(\sigma + 2it) \geq 0.$$

BEWEIS. Für $\theta \in \mathbb{R}$ sei $V(\theta) = 3 + 4\cos(\theta) + \cos(2\theta)$. Man hat

$$V(\theta) = 3 + 4\cos(\theta) + 2\cos^2(\theta) - 1 = 2(1 + \cos(\theta))^2.$$

Damit ist $V(\theta) \geq 0$. Die linke Seite unserer behaupteten Ungleichung ist gegeben durch

$$\sum_{n=1}^{\infty} a_n n^{-\sigma} V(t \log(n)).$$

Daraus folgt die Behauptung. □

KOROLLAR 3.5.2. *Für $\sigma > 1$ gilt*

$$\zeta(\sigma)^3 |\zeta(\sigma + it)|^4 |\zeta(\sigma + 2it)| \geq 1.$$

BEWEIS. Man wendet den obigen Satz an auf die Funktion

$$F(s) = \log(\zeta(s)) = - \sum_p \log(1 - p^{-s}) = \sum_{n \geq 2} \frac{\Lambda(n)}{\log(n)} n^{-s}.$$

Diese konvergiert für $\sigma > 1$. Mit exp folgt die Behauptung. □

Nun können wir folgenden Satz beweisen:

THEOREM 3.5.3. *Die Funktion $\zeta(s)$ hat keine Nullstelle in der Halbebene $\sigma \geq 1$.*

BEWEIS. Wir müssen nur noch den Fall $\sigma = 1$ betrachten. Angenommen, $\zeta(1 + it) = 0$. Dann ist $t \neq 0$. Wegen Korollar 3.5.2 gilt für $\sigma > 1$

$$((\sigma - 1)\zeta(\sigma))^3 \left| \frac{\zeta(\sigma + it)}{\sigma - 1} \right|^4 |\zeta(\sigma + 2it)| \geq \frac{1}{\sigma - 1}.$$

Was passiert, wenn wir dort $\sigma \rightarrow 1+$ gehen lassen? Der erste Faktor geht gegen 1, weil $\zeta(s)$ das Residuum 1 hat am Pol $s = 1$. Der dritte Faktor geht gegen $|\zeta(1 + 2it)|$. Für den mittleren Faktor hätte man

$$\left| \frac{\zeta(\sigma + it)}{\sigma - 1} \right|^4 = \left| \frac{\zeta(\sigma + it) - \zeta(1 + it)}{\sigma - 1} \right|^4 \rightarrow |\zeta'(1 + it)|^4$$

für $\sigma \rightarrow 1+$. Insgesamt ginge die linke Seite also gegen $|\zeta'(1 + it)|^4 |\zeta(1 + 2it)|$, die rechte Seite aber gegen ∞ für $\sigma \rightarrow 1+$. Das ist ein Widerspruch. \square

Aus der Funktionalgleichung folgt nun:

KOROLLAR 3.5.4. *Die einzigen Nullstellen von $\zeta(s)$ in der Halbebene $\sigma \leq 0$ sind die trivialen Nullstellen bei $s = -2n$, welche einfache Pole sind.*

Die Zetafunktion hat außer den trivialen Nullstellen keine Nullstellen auf der reellen Achse.

LEMMA 3.5.5. *Für $\sigma > 0$ gilt*

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

Das impliziert $\zeta(\sigma) < 0$ für $0 < \sigma < 1$. Insbesondere ist $\zeta(\sigma) = 0$ dort unmöglich.

BEWEIS. Für $\sigma > 1$ gilt

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

Die Reihe auf der rechten Seite konvergiert auch für $\sigma > 0$, so daß die Identität für $\sigma > 0$ gültig ist (durch analytische Fortsetzung). Für reelles s hat die alternierende Reihe eine positive Summe. Für $0 < \sigma < 1$ ist der Faktor $1 - 2^{1-\sigma}$ negativ, so daß auch $\zeta(\sigma)$ negativ ist. \square

Der sogenannte *kritische Streifen* ist die Menge der $s \in \mathbb{C}$ mit $0 < \sigma < 1$. Dort hat $\zeta(s)$ unendlich viele (nicht-reelle) Nullstellen. In der Tat, sei $N(T)$ die Anzahl der Nullstellen von $\zeta(s)$ im Bereich $0 < \sigma < 1$, $0 < t \leq T$. Dann gilt folgende Formel, die Riemann-von Mangoldt

Formel

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

Also hat $\zeta(s)$ unendlich viele Nullstellen im kritischen Streifen. Sie liegen symmetrisch bezüglich der reellen Achse und der *kritischen Geraden* $\sigma = \frac{1}{2}$. Die **Riemannsche Vermutung** besagt, daß alle diese nicht-trivialen Nullstellen auf der kritischen Geraden liegen. Extensive numerische Berechnungen sprechen für die Wahrheit dieser Behauptung, aber einen Beweis gibt es bisher nicht. Es ist bekannt, daß zumindest $\frac{2}{5}$ aller nicht-trivialer Nullstellen auf der kritischen Geraden liegen. Die Suche nach dem Beweis ist so etwas wie die Suche nach dem heiligen Gral. Die *verallgemeinerte Riemannsche Vermutung* besagt, daß außerdem alle nicht-trivialen Nullstellen von $L(s, \chi)$ auf der kritischen Geraden liegen. Noch allgemeiner kann man das für alle automorphen L -Funktionen vermuten. Es gäbe noch sehr viel zu sagen dazu, und man kann auf die Zukunft gespannt sein - wir schließen nun aber, und zwar mit einem Bild von Bernhard Riemann.



Bibliography

- [1] T. Apostol: *Introduction to analytic number theory*. Springer Verlag, fünfte Auflage (1998).
- [2] J. Brüderin: *Einführung in die analytische Zahlentheorie*. Springer-Verlag (1995).
- [3] E. D. Cashwell, C. J. Everett: *The ring of number-theoretic functions*. Pacific J. Math. **9** (1959), 975-985.
- [4] P. L. Chebyshev: *Mémoire sur les nombres premiers*. Journal de Math. Pures et Appl. **17** (1852), 366-390.
- [5] P. Dusart: *Inégalités explicites pour $\psi(X)$, $\theta(X)$, $\pi(X)$ et les nombres premiers..* C. R. Math. Acad. Sci. Soc. R. Can. **21** (1999), no. 2, 53-59.
- [6] P. Dusart: *The k th prime is greater than $k(\ln k + \ln \ln k - 1)$ for $k \geq 2$* . Math. Comp. **68** (1999), no. 225, 411-415.
- [7] P. Dusart: *Atour de la fonction qui compte le nombre de nombres premiers*. Thèse de Doctorat de l'Université de Limoges (1998).
- [8] W. and F. Ellison: *Prime numbers*. Wiley Interscience **1985**.
- [9] D. R. Heath-Brown, S. J. Patterson: *The distribution of Kummer sums at prime arguments*. J. reine angew. Math. **310** (1979), 111-130.
- [10] K. F. Ireland; M. I. Rosen: *A classical introduction to modern number theory*. Graduate Texts in Mathematics **84**. Springer-Verlag, New York-Berlin (1982).
- [11] C. Khare: *On Serre's modularity conjecture for 2-dimensional mod p representations of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ unramified outside p* . Arxiv math.NT/0504080.
- [12] C. R. Matthews: *Gauß-Sums and Elliptic Functions*. Invent. Math. **52**, no. 2 (1979), 163-185.
- [13] D. J. Newman, *Analytic number theory*. Graduate Texts in Mathematics **177** (1998).
- [14] A. M. Odlyzko, H. J. te Riele, *Disproof of the Mertens Conjecture*. J. reine angew. Math. **357** (1985), 138-160.
- [15] H. N. Shapiro, *On the number of primes less than or equal x* . Proc. Amer. Math. Soc. **1** (1950), 346-348.
- [16] G. Tenenbaum: *Introduction to analytic and probabilistic number theory*. Cambridge studies in advanced mathematics **46** (1995).
- [17] D. Zagier: *Newman's short proof of the prime number theorem*. Amer. Math. Monthly **104**, No. 8 (1997), 705-708.