Studienbücherei

E. Krätzel
Zahlentheorie

VEB Deutscher Verlag der Wissenschaften

Mathematik für Lehrer
Band 19

Herausgegeben von:
W. Engel, S. Brehmer, M. Schneider, H. Wussing

Unter Mitarbeit von:
G. Asser, J. Böhm, J. Flachsmeyer, G. Geise, T. Glocke,
K. Härtig, G. Kasdorf, O. Krötenheerdt, H. Lugowski,
P. H. Müller, G. Porath

Studienbücherei

Zahlentheorie

E. Krätzel

Mit 3 Abbildungen

VEB Deutscher Verlag
der Wissenschaften
Berlin 1981

Verlagslektoren: Erika Arndt, Karin Bratz
Verlagshersteller: Ilona Hoffmann
Umschlaggestaltung: Rudolph Wendt

Lizenznummer: 206 · 435/74/81
Printed in the German Democratic Republic
Gesamtherstellung: VEB Druckhaus „Maxim Gorki", 7400 Altenburg
LSV 1054
Bestellnummer: 570 965 4
DDR 19,80 M

Vorwort

Das vorliegende Buch ist aus Vorlesungen entstanden, die ich mehrfach im Rahmen der wahlweise-obligatorischen Ausbildung vor Lehrerstudenten an der Friedrich-Schiller-Universität in Jena gehalten habe. Die Beschäftigung mit den Zahlen beeinflußt in bedeutender Weise einen jeden Mathematikunterricht von der ersten Klasse bis zum letzten Schuljahr. Somit soll dieses Buch dem zukünftigen Mathematiklehrer einen tieferen Einblick in das Reich der Zahlen vermitteln als dies im Grundkurs Mathematik möglich sein kann. Dabei galt es, in der Stoffauswahl einmal hinreichend breit, zum anderen an einzelnen Stellen auch genügend tief zu bleiben. Der Überblickscharakter sollte gewahrt sein durch eine ausführliche Behandlung der Teilbarkeitslehre, durch die Aufnahme abstrakter, struktureller Gesichtspunkte, durch Approximationsprobleme bei reellen Zahlen sowie eine ausgedehnte Behandlung der zahlentheoretischen Funktionen und Gitterpunktprobleme. Die Darstellung der Theorie der diophantischen Gleichungen erfolgte fast ausschließlich im Gewand der Gitterpunktlehre, um bei Heranziehung geometrischer Gesichtspunkte größere Anschaulichkeit zu erzielen. Vertiefungen erfolgten bei der Behandlung des quadratischen Reziprozitätsgesetzes mit Gaußschen Summen, der Transzendenzbeweise von e und π, der Darlegung einer elementaren Variante des Beweises des Primzahlsatzes und der elementaren Vinogradovschen Methode zur Abschätzung von Gitterpunkten. Natürlich wird es kaum möglich sein, in einer Lehrveranstaltung alle diese schwierigen Probleme abzuhandeln. Aber ich denke, ein Mathematiklehrer sollte auch einmal einen Transzendenzbeweis studieren und bei der einen oder anderen zahlentheoretischen Fragestellung etwas länger verweilen. Übrigens liegt inzwischen eine ganze Reihe von Varianten des elementaren Beweises des Primzahlsatzes vor. Daß hier auf die in [7] dargestellte Wrightsche Modifikation zurückgegriffen wurde, hat ausschließlich den Grund, daß dieses Vorgehen der Anlage des Kapitels 5 am besten entspricht.

Den einzelnen Kapiteln wurden Aufgaben beigegeben, die teilweise reinen Übungscharakter, teilweise auch weiterführenden Charakter tragen. Im allgemeinen sind sie nicht zu schwierig und mit den bereitgestellten Hilfsmitteln in ansprechender Zeit zu lösen. Aufgaben, die Anspruch auf Originalität haben, sind namentlich gekennzeichnet. Sie müssen deshalb nicht schwierig sein!

Meine Mitarbeiter, Herr Dr. MENZER und Herr SCHNABEL, haben das Manuskript kritisch durchgesehen und durch viele Hinweise zur Verbesserung beigetragen. Ich bin ihnen sehr zu Dank verpflichtet.

Jena, 1981 EKKEHARD KRÄTZEL

Inhalt

1.	**Der Fundamentalsatz der Zahlentheorie**	9
1.1.	Teilbarkeit und Primzahlen	9
1.2.	Darstellung der natürlichen Zahlen als Produkte von Primzahlen	11
1.3.	Der größte gemeinsame Teiler und das kleinste gemeinsame Vielfache	12
1.4.	Aufgaben	15
2.	**Kongruenzen**	17
2.1.	Der Restklassenring	17
2.2.	Die prime Restklassengruppe	20
2.3.	Lineare diophantische Gleichungen	24
2.4.	Simultane lineare Kongruenzen	25
2.5.	Die Struktur der primen Restklassengruppe	26
2.6.	Die Indexrechnung	31
2.7.	Potenzreste	33
2.8.	Quadratische Kongruenzen	36
2.9.	Aufgaben	43
3.	**Endliche abelsche Gruppen**	45
3.1.	Nicht-isomorphe endliche abelsche Gruppen	45
3.2.	Charaktere endlicher abelscher Gruppen	48
3.3.	Restklassencharaktere	50
3.4.	Gaußsche Summen	52
3.5.	Das quadratische Reziprozitätsgesetz im Lichte der Gaußschen Summen	55
3.6.	Aufgaben	64
4.	**Algebraische und transzendente Zahlen**	65
4.1.	Die Entwicklung reeller Zahlen in Kettenbrüche	65
4.2.	Approximation reeller Zahlen durch rationale Zahlen	73
4.3.	Algebraische Zahlen	77
4.4.	Transzendente Zahlen	78
4.5.	Die Irrationalität von e und π	80
4.6.	Die Transzendenz von e und π	81
4.7.	Aufgaben	86
5.	**Zahlentheoretische Funktionen**	87
5.1.	Dirichletsche Multiplikation zahlentheoretischer Funktionen	87
5.2.	Dirichletsche Reihen	92
5.3.	Abschätzungen von Summen	97
5.4.	Die Primzahlfunktion	101
5.4.1.	Der Euklidische Beweis der Unendlichkeit der Menge der Primzahlen	101

5.4.2. Einfache Abschätzungen der Primzahlfunktion 103
5.4.3. Die Ergebnisse von ČEBYŠEV 106
5.4.4. Die Selbergsche Formel 112
5.4.5. Elementarer Beweis des Primzahlsatzes 116
5.5. Die maximale Größenordnung zahlentheoretischer Funktionen 121
5.5.1. Die Teilerfunktionen 121
5.5.2. Die Eulersche φ-Funktion 127
5.5.3. Die Anzahl der Primfaktoren natürlicher Zahlen 128
5.6. Ramanujansche Reihen 129
5.7. Die durchschnittliche Größenordnung zahlentheoretischer Funktionen 132
5.7.1. Die Eulersche φ-Funktion 132
5.7.2. Quadratsummen 133
5.7.3. Die Teilerfunktionen 134
5.7.4. Quadratfreie Zahlen 136
5.7.5. Die Anzahl der Primfaktoren natürlicher Zahlen 136
5.7.6. Die Möbiussche μ-Funktion und der Primzahlsatz 140
5.8. Die normale Größenordnung zahlentheoretischer Funktionen 143
5.9. Aufgaben 146

6. Gitterpunkte 149

6.1. Gitterpunkte auf Kurven zweiter Ordnung 149
6.1.1. Gitterpunkte auf Parabeln 150
6.1.2. Gitterpunkte auf Ellipsen 151
6.1.3. Gitterpunkte auf Hyperbeln 153
6.2. Darstellungen natürlicher Zahlen als Summe von Quadraten 162
6.3. Rationale Punkte auf Kurven zweiter Ordnung 170
6.4. Spezielle diophantische Gleichungen dritten und vierten Grades 176
6.5. Gitterpunkte in ebenen Bereichen 179
6.5.1. Gitterpunkte in allgemeinen Bereichen 180
6.5.2. Die Methode von VINOGRADOV 182
6.5.3. Das Kreisproblem und Verallgemeinerungen 190
6.5.4. Das Teilerproblem und Verallgemeinerungen 194
6.6. Gitterpunkte in mehrdimensionalen Kugeln 197
6.7. Aufgaben 200

7. Partitionen 201

7.1. Elementare Eigenschaften 201
7.2. Abschätzungen und asymptotische Darstellungen 205
7.3. Die Anzahl der nicht-isomorphen abelschen Gruppen n-ter Ordnung 209
7.4. Aufgaben 215

Literatur 217

Namen- und Sachverzeichnis 218

1. Der Fundamentalsatz der Zahlentheorie

Die elementare Zahlentheorie beschäftigt sich vornehmlich mit den natürlichen Zahlen. Über diese setzen wir die Kenntnis der Gesetze der elementaren Rechenoperationen und der Anordnung als bekannt voraus. Wir berufen uns ferner auf das Prinzip der vollständigen Induktion und das Prinzip der kleinsten Zahl, nach dem jede nichtleere Menge von natürlichen Zahlen eine eindeutig bestimmte kleinste Zahl enthält. Ebenso nehmen wir die Erweiterung des Bereiches $\mathbf{N}$ der natürlichen Zahlen zum Integritätsbereich $\mathbf{Z}$ der ganzen Zahlen als gegeben hin. In diesem Kapitel entwickeln wir die grundlegende Begriffsbildung der elementaren Zahlentheorie, die Teilbarkeit. Als wesentliche Grundlage für den multiplikativen Aufbau der ganzen Zahlen werden sich dabei die Primzahlen hervorheben. Das wichtigste Ergebnis wird der Fundamentalsatz der Zahlentheorie sein, nach dem sich jede natürliche Zahl im wesentlichen eindeutig als Produkt von Primzahlen darstellen läßt. Es sei noch darauf hingewiesen, daß Teile der elementaren Teilbarkeitslehre bereits in MfL, Bd. 1 behandelt wurden.

1.1. Teilbarkeit und Primzahlen

Definition 1.1. Die ganze Zahl t heißt ein *Teiler* der ganzen Zahl n, wenn es eine ganze Zahl g gibt mit $n = t \cdot g$.

Ist t ein Teiler von n, so werden wir $t \mid n$ schreiben. Ist dagegen t kein Teiler von n, so werden wir dies durch $t \nmid n$ ausdrücken.

Die folgenden einfachen Teilbarkeitsbeziehungen ergeben sich unmittelbar aus der Definition und den Eigenschaften von $\mathbf{Z}$:

$$1 \mid n, \qquad n \mid n, \qquad n \mid 0,$$
$$0 \mid n \Rightarrow n = 0,$$
$$t \mid n \wedge n \mid m \Rightarrow t \mid m,$$
$$t \mid n \wedge t \mid m \Rightarrow t \mid (an + bm),$$
$$t \mid n \Rightarrow at \mid an,$$
$$at \mid an \wedge a \neq 0 \Rightarrow t \mid n,$$
$$t \mid n \wedge n \neq 0 \Rightarrow |t| \leqq |n|,$$
$$t \mid d \wedge d \mid t \Rightarrow |t| = |d|,$$
$$t \mid n \wedge d = \frac{n}{t} \Rightarrow d \mid n.$$

Eine jede von 0 verschiedene ganze Zahl n besitzt die Teiler ± 1, $\pm n$, welche wir die trivialen Teiler nennen wollen. Die Zahlen ± 1 werden die Einheiten von $\mathbf{Z}$ genannt. Sie sind dadurch gekennzeichnet, daß auch ihre reziproken Werte zu $\mathbf{Z}$ gehören. Ebenso folgt aus $t \mid n$ stets $(\pm t) \mid (\pm n)$. Man sieht also, daß es bei Teilbarkeitsaussagen nicht auf Einheiten ankommt und man sich demzufolge auf den Bereich $\mathbf{N}$ der natürlichen Zahlen beschränken kann. Wir wollen dabei vereinbaren, daß 0 nicht zu $\mathbf{N}$ gerechnet wird.

Definition 1.2. Eine natürliche Zahl $p > 1$ heißt *Primzahl*, wenn sie nur durch 1 und sich selbst teilbar ist.

Die Übereinkunft, 1 nicht zu den Primzahlen zu rechnen, erweist sich für die Formulierung vieler zahlentheoretischer Gesetzmäßigkeiten als zweckmäßig. Damit beginnt die Folge der Primzahlen mit 2, 3, 5, 7, 11, ..., in der 2 die einzige gerade Primzahl darstellt. Eine natürliche Zahl $n > 1$, die keine Primzahl ist, werden wir eine *zusammengesetzte Zahl* nennen.

Satz 1.1. *Jede natürliche Zahl $n > 1$ besitzt mindestens einen Primteiler, das heißt eine Primzahl p mit $p \mid n$.*

Beweis. Wir betrachten die Menge

$$A := \{a : a \in \mathbf{N},\ a > 1,\ a \mid n\}.$$

Wegen $n \mid n$ ist A nicht leer und besitzt daher eine kleinste Zahl p. Diese Zahl ist Primzahl. Denn gäbe es eine Zahl q mit $q \mid p$ und $1 < q < p$, so wäre auch $q \mid n$. Dies steht aber im Widerspruch zur Auswahl von p als kleinstem Teiler von n.

Bereits in den „Elementen" von Euklid (etwa 365—300 v. u. Z.) findet sich der Nachweis der Unendlichkeit der Menge der Primzahlen.

Satz 1.2. *Es gibt unendlich viele Primzahlen.*

Beweis. Im Gegensatz zur Behauptung nehmen wir an, es gibt nur endlich viele Primzahlen. Wir notieren sie uns der Reihe nach, schreiben $2 = p_1$, $3 = p_2$, ..., p_n und bilden die Zahl

$$P = p_1 p_2 \cdot \cdots \cdot p_n + 1.$$

Nach Satz 1.1 gibt es eine Primzahl p mit $p \mid P$. Diese ist von $p_1, p_2, \ldots, p_n$ verschieden, denn sonst wäre $p \mid p_1 p_2 \cdot \cdots \cdot p_n$ und damit auch $p \mid 1$, was aber nicht möglich sein kann.

Die Primzahlen scheinen in der Folge der natürlichen Zahlen völlig unregelmäßig verteilt zu sein. Einerseits kann man beliebig große Lücken feststellen. Ist $n > 1$ eine beliebige natürliche Zahl, so befindet sich unter den aufeinanderfolgenden Zahlen $n! + 2$, $n! + 3$, ..., $n! + n$ keine einzige Primzahl, da in ihnen nacheinander die Zahlen 2, 3, ..., n als echte Teiler enthalten sind. Andererseits trifft man immer wieder auf die sogenannten *Primzahlzwillinge*, das sind Paare $(p, p + 2)$ von Primzahlen, die sich nur durch die Differenz 2 unterscheiden. Die ersten Primzahlzwillinge sind (3, 5), (5, 7), (11, 13), (17, 19). Es ist zwar gegenwärtig noch nicht bekannt, ob es unendlich viele Primzahlzwillinge gibt oder nicht, dennoch suggerieren die beiden genannten Tatsachen ein totales Chaos in der Verteilung der Primzahlen. Daß dies

aber nicht so ist, werden wir im Kapitel 5 kennenlernen. Aus diesem Grunde sollte man die folgende *Abschätzung der n-ten Primzahl*, die sich aus dem Euklidischen Beweis des Satzes 1.2 ergibt, auch wenn sie noch so grob ist, nicht unterschätzen. Bezeichnet p_n die n-te Primzahl, also $p_1 = 2$, $p_2 = 3$ usw., so gilt

$$p_n \leqq 2^{2^{n-1}}.$$

Diese Abschätzung ist für $n = 1$ sicher richtig. Weiter folgt nach dem Euklidischen Beweisverfahren durch Induktion von $n - 1$ auf n

$$\begin{aligned} p_n &\leqq p_1 p_2 \cdot \cdots \cdot p_{n-1} + 1 \\ &\leqq 2^{2^0 + 2^1 + \cdots + 2^{n-2}} + 1 = 2^{2^{n-1}-1} + 1 \leqq 2^{2^{n-1}}. \end{aligned}$$

1.2. Darstellung der natürlichen Zahlen als Produkte von Primzahlen

Nach Satz 1.1 läßt sich jede natürliche Zahl $n > 1$ als ein Produkt von Primzahlen darstellen. Denn n enthält wenigstens einen Primteiler p_1 und besitzt daher eine Darstellung $n = p_1 n_1$. Für $n_1 = 1$ ist die Behauptung gegeben. Für $n_1 > 1$ gibt es einen Primteiler p_2 von n_1. Damit ist $n_1 = p_2 n_2$ und $n = p_1 p_2 n_2$. In Fortsetzung des Verfahrens erhält man $n = p_1 p_2 \cdot \cdots \cdot p_k n_k$ mit den Primzahlen $p_1, p_2, \ldots, p_k$ und der natürlichen Zahl n_k. Ist $n_k = 1$, so ist das Verfahren an dieser Stelle beendet, für $n_k > 1$ setze man es entsprechend fort. Man erhält auf diese Weise eine streng monoton fallende Folge von natürlichen Zahlen n_k, so daß das Verfahren nach endlich vielen Schritten abbrechen muß. Das sei an der Stelle $k = r$ der Fall, womit die Primfaktorzerlegung $n = p_1 p_2 \cdot \cdots \cdot p_r$ gefunden ist.

Von größter Bedeutung ist nun, daß die Zerlegung von n in Primfaktoren, abgesehen von der Reihenfolge, eindeutig ist. Für diese fundamentale Tatsache ist eine Reihe von Beweisen bekannt. Wir wählen einen Beweis aus, der im Jahre 1962 von J. Surányi gegeben wurde. Dabei wird die Existenz einer Primfaktorzerlegung gleich noch einmal mitbewiesen.

Satz 1.3 (Fundamentalsatz der Zahlentheorie). *Jede natürliche Zahl $n > 1$ läßt sich als Produkt von Primzahlen darstellen, wobei die Darstellung bis auf die Reihenfolge der Faktoren eindeutig ist.*

Beweis. Der Satz gilt für 2 und jede weitere Primzahl. Es sei daher n eine zusammengesetzte Zahl, und wir nehmen die Richtigkeit des Satzes für alle natürlichen Zahlen kleiner als n an. Dann gibt es natürliche Zahlen a, b mit $n = ab$ und $1 < a \leqq b < n$. Da der Satz für a und b gilt, geben die Primfaktorzerlegungen von a und b eine Primfaktorzerlegung von n.

Der kleinste Teiler $p > 1$ von n ist natürlich eine Primzahl. Wenn wir zeigen können, daß p unter den Primfaktoren von a oder b vorkommt, so ist auch die Eindeutigkeit der Primfaktorzerlegung von n nachgewiesen. Denn nach Induktionsannahme hat die Zahl $n' = n / p$ wegen $n' < n$ eine eindeutige Primfaktorzerlegung.

Es ist $p \leqq a$, da p der kleinste Teiler von n ist. Für $p = a$ gilt unsere Behauptung. Für $p < a$ bilden wir mit $a' = a - p$ die Zahl $n'' = a'b = (a - p)\, b = n - pb$. Da-

mit ist $p \mid n''$, $0 < n'' < n$, und n'' besitzt eine eindeutige Primfaktorzerlegung, die aus den Zerlegungen von a' und b resultiert. Folglich muß p unter Primfaktoren von a' oder b vorkommen. Ist p in b enthalten, so sind wir fertig. Ist a' durch p teilbar, so auch $a = a' + p$. Somit ist auch in diesem Fall der Beweis beendet.

Üblicherweise faßt man in der Primfaktorzerlegung $n = p_1 p_2 \cdot \cdots \cdot p_r$ gleiche Primzahlen zu Primzahlpotenzen zusammen und spricht

$$n = \prod_{i=1}^{k} p_i^{\nu_i}$$

mit $p_1 < p_2 < \cdots < p_k$, $\nu_i \geqq 1$ als die *kanonische Zerlegung* von n an. Manchmal ist auch die folgende Darstellung ganz nützlich:

$$n = \prod_{p} p^{\nu_p}.$$

Dabei ist das Produkt über alle Primzahlen p zu erstrecken. Für jedes p ist $\nu_p \geqq 0$, aber nur für endlich viele p soll $\nu_p > 0$ sein.

Den Anfänger mag der Wert, der dem Fundamentalsatz der Zahlentheorie beigemessen wird, zunächst befremden, nimmt er doch die eindeutige Primfaktorzerlegung einer natürlichen Zahl aus dem Schulunterricht als selbstverständlich gegeben hin. Es sei aber darauf verwiesen, daß der zugrunde gelegte Zahlenbereich hierbei die entscheidende Rolle spielt. Mit derselben Berechtigung wie in $\mathbf{Z}$ beziehungsweise $\mathbf{N}$ kann auch in andereren Zahlenbereichen, wie etwa im Bereich der komplexen Zahlen, in sinnvoller Weise Zahlentheorie betrieben werden. Es stellt sich dann heraus, daß ein solcher Satz von der eindeutigen Primfaktorzerlegung im allgemeinen keine Gültigkeit mehr hat. Es würde den Rahmen dieses Buches sprengen, auf solche allgemeineren Zahlenbereiche einzugehen. Statt dessen soll als einfaches, aber instruktives Beispiel die Teilmenge der natürlichen Zahlen

$$\mathbf{M} := \{m : m \in \mathbf{N},\ m = 4n + 1,\ n = 0, 1, \ldots\}$$

betrachtet werden. Eine Primzahl wird in $\mathbf{M}$ genau wie in $\mathbf{N}$ erklärt. Demzufolge sind die ersten sieben Primzahlen die Zahlen 5, 9, 13, 17, 21, 29, 33. Daß in $\mathbf{M}$ der Satz von der eindeutigen Primfaktorzerlegung nicht gilt, kann leicht durch ein Beispiel belegt werden. Die Zahl 693 besitzt in $\mathbf{M}$ die beiden verschiedenen Zerlegungen $693 = 9 \cdot 77 = 21 \cdot 33$, wobei die Zahlen 9, 21, 33, 77 sämtlich Primzahlen in $\mathbf{M}$ sind.

1.3. Der größte gemeinsame Teiler und das kleinste gemeinsame Vielfache

Sind a, b natürliche Zahlen mit den Darstellungen

$$a = \prod_{p} p^{\alpha_p}, \quad b = \prod_{p} p^{\beta_p},$$

so ist offensichtlich $b \mid a$ genau dann, wenn $\beta_p \leqq \alpha_p$ für alle p ist. Betrachten wir jetzt gemeinsame Teiler endlich vieler Zahlen. Es seien $a_1, a_2, \ldots, a_n$ ganze Zahlen, wobei

etwa die Zahlen $a_1, a_2, \ldots, a_r$ mit $1 \leqq r \leqq n$ von 0 verschieden sein sollen. Für diese Zahlen haben wir die Darstellungen

$$|a_k| = \prod_p p^{\nu_{p,k}} \qquad (k = 1, 2, \ldots, r). \tag{1}$$

Die Zahlen x mit

$$|x| = \prod_p p^{\nu_p}$$

und $\nu_p \leqq \nu_{p,k}$ $(k = 1, 2, \ldots, r)$ bilden die gemeinsamen Teiler von $a_1, a_2, \ldots, a_n$. Unter ihnen befindet sich die natürliche Zahl

$$d = \prod_p p^{m_p}$$

mit

$$m_p = \min(\nu_{p,1}, \nu_{p,2}, \ldots, \nu_{p,r}).$$

Sie ist nicht nur gemeinsamer Teiler von $a_1, a_2, \ldots, a_n$, sondern jeder gemeinsame Teiler dieser Zahlen ist sogar ein Teiler von d. Sie erfüllt also die beiden Eigenschaften

$$d \mid a_k \quad \text{für} \quad k = 1, 2, \ldots, n, \tag{2}$$

$$t \mid a_k \quad \text{für} \quad k = 1, 2, \ldots, n \Rightarrow t \mid d. \tag{3}$$

Überdies ist d eindeutig bestimmt. Dies führt zu folgender Festlegung:

Definition 1.3. Die zu den ganzen Zahlen $a_1, a_2, \ldots, a_n$, die nicht sämtlich 0 sind, durch die Eigenschaften (2) und (3) eindeutig bestimmte natürliche Zahl d heißt der *größte gemeinsame Teiler* dieser Zahlen.

Wir können auch den Fall $a_1 = a_2 = \cdots = a_n = 0$ einbeziehen, wenn wir hierfür $d = 0$ setzen. Es wird allgemein die Schreibweise

$$d = (a_1, a_2, \ldots, a_n)$$

benutzt (man beachte hierzu auch [2]). Für $d = 1$ nennen wir die Zahlen $a_1, a_2, \ldots, a_n$ teilerfremd. Aus der Darstellung des größten gemeinsamen Teilers liest man ohne weiteres

$$(a_1, a_2, \ldots, a_{n-1}, a_n) = \big((a_1, a_2, \ldots, a_{n-1}), a_n\big)$$

ab, so daß die Bestimmung des größten gemeinsamen Teilers von n Zahlen auf die von zwei Zahlen zurückgeführt ist.

Jetzt ziehen wir gemeinsame Vielfache von endlich vielen Zahlen in Betracht. Es seien die ganzen Zahlen $a_1, a_2, \ldots, a_n$ sämtlich von 0 verschieden. Wir nutzen wieder die Darstellungen (1) mit $r = n$. Die Zahlen y mit

$$|y| = \prod_p p^{\nu_p}$$

und $\nu_p \geqq \nu_{p,k}$ $(k = 1, 2, \ldots, n)$ bilden die gemeinsamen Vielfachen von $a_1, a_2, \ldots, a_n$. Unter ihnen befindet sich die natürliche Zahl

$$v = \prod_p p^{M_p}$$

mit

$$M_p = \max(\nu_{p,1}, \nu_{p,2}, \ldots, \nu_{p,n}).$$

Sie ist nicht nur gemeinsames Vielfaches von $a_1, a_2, \ldots, a_n$, sondern jedes Vielfache dieser Zahlen ist auch ein Vielfaches von v. Damit genügt v den Eigenschaften

$$a_k \mid v \quad \text{für} \quad k = 1, 2, \ldots, n, \tag{4}$$

$$a_k \mid w \quad \text{für} \quad k = 1, 2, \ldots, n \Rightarrow v \mid w. \tag{5}$$

Natürlich ist v eindeutig bestimmt. Somit legen wir fest:

Definition 1.4. Die zu den ganzen Zahlen $a_1, a_2, \ldots, a_n$, die sämtlich von 0 verschieden sind, durch die Eigenschaften (4) und (5) eindeutig bestimmte natürliche Zahl $v := [a_1, a_2, \ldots, a_n]$ heißt *kleinstes gemeinsames Vielfaches* dieser Zahlen.

Ist eine der Zahlen $a_k = 0$, so legen wir hierfür $v = 0$ fest.

Zwischen dem größten gemeinsamen Teiler und dem kleinsten gemeinsamen Vielfachen zweier natürlicher Zahlen a, b besteht ein einfacher Zusammenhang. Aus den Darstellungen für d und v entnimmt man

$$(a, b)\,[a, b] = ab.$$

Das Problem der Bestimmung des größten gemeinsamen Teilers von zwei natürlichen Zahlen kann ohne Zuhilfenahme ihrer Primfaktorzerlegung gelöst werden. Hierzu benutzen wir das als *Euklidischer Algorithmus* bekannte Verfahren. Es seien $a_0, a_1 \in \mathbf{N}$ mit $a_0 > a_1 > 1$. Gesucht ist der größte gemeinsame Teiler $d = (a_0, a_1)$. Der Algorithmus besteht in einer fortwährenden *Division mit Rest* (siehe [2]), wie sich aus nachstehendem Schema, in dem alle aufgeführten Zahlen ganz sind, unmittelbar ergibt:

$$\begin{aligned}
a_0 &= a_1 q_1 + a_2, & 0 < a_2 < a_1,\\
a_1 &= a_2 q_2 + a_3, & 0 < a_3 < a_2,\\
&\ldots\ldots\ldots & \ldots\ldots\ldots\\
a_{n-2} &= a_{n-1} q_{n-1} + a_n, & 0 < a_n < a_{n-1},\\
a_{n-1} &= a_n q_n, & 0 = a_{n+1}.
\end{aligned}$$

Der Divisionsalgorithmus findet nach endlich vielen Schritten seinen Abschluß, da die Folge der Reste $a_2, a_3, \ldots$ eine streng monoton fallende Folge nichtnegativer ganzer Zahlen bildet, die nach unten beschränkt ist. Der letzte von 0 verschiedene Rest a_n ist der gesuchte größte gemeinsame Teiler $a_n = (a_0, a_1)$. Durchläuft man nämlich die Gleichungskette von unten nach oben, so erkennt man nacheinander

$$a_n \mid a_{n-1} \Rightarrow a_n \mid a_{n-2} \Rightarrow \cdots \Rightarrow a_n \mid a_1 \Rightarrow a_n \mid a_0.$$

Das ist aber die Eigenschaft (1) in der Definition 1.3. Zur Überprüfung der Eigenschaft (2) sei $t \mid a_0$ und $t \mid a_1$. Dann ergibt sich beim Durchlaufen der Gleichungskette

von oben nach unten

$$t \mid a_0 \wedge t \mid a_1 \Rightarrow t \mid a_2 \Rightarrow t \mid a_3 \Rightarrow \cdots \Rightarrow t \mid a_n .$$

Aus dem Euklidischen Algorithmus folgt noch die bemerkenswerte Tatsache, daß sich der größte gemeinsame Teiler von n Zahlen aus diesen linear kombinieren läßt.

Satz 1.4. *Ist $d = (c_1, c_2, \ldots, c_n)$ der größte gemeinsame Teiler von n ganzen Zahlen, so existieren n ganze Zahlen $x_1, x_2, \ldots, x_n$ mit*

$$d = c_1 x_1 + c_2 x_2 + \cdots + c_n x_n . \tag{6}$$

Beweis. Wir führen den Beweis zunächst für $n = 2$. Ist eine der beiden Zahlen c_1, c_2 gleich 0, so ist die Aussage des Satzes trivial. Wir können also c_1, c_2 als natürliche Zahlen annehmen und außerdem $c_1 > c_2$. Wir setzen $c_1 = a_0, c_2 = a_1$ und durchlaufen obige Gleichungskette des Euklidischen Algorithmus von oben nach unten. Mit ganzen Zahlen ξ_k, η_k erhalten wir

$$\begin{aligned}
a_2 &= a_0 - a_1 q_1 = a_0 \xi_2 + a_1 \eta_2 , \\
a_3 &= a_1 - a_2 q_2 = a_0 \xi_3 + a_1 \eta_3 , \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
a_n &= a_{n-2} - a_{n-1} q_{n-1} = a_0 \quad \xi_n + a_1 \eta_n .
\end{aligned}$$

Mit $\xi_n = x_1$, $\eta_n = x_2$ ergibt sich hieraus $d = c_1 x_1 + c_2 x_2$.

Für beliebiges n ergibt sich der Satz durch Induktion. Es sei (6) für n richtig. Für $n + 1$ haben wir

$$\begin{aligned}
(c_1, c_2, \ldots, c_n, c_{n+1}) &= \big((c_1, c_2, \ldots, c_n), c_{n+1}\big) \\
&= (c_1, c_2, \ldots, c_n)\, x + c_{n+1} x_{n+1} \\
&= c_1 (x x_1) + c_2 (x x_2) + \cdots + c_n (x x_n) + c_{n+1} x_{n+1} .
\end{aligned}$$

Daraus ergibt sich die Behauptung.

1.4. Aufgaben

1. Man zeige: Die Summe von Primzahlzwillingen $p, p + 2$ mit $p > 3$ ist stets durch 12 teilbar.
2. Man zeige: Ist n eine nicht durch 2 und 3 teilbare natürliche Zahl, so ist stets 24 ein Teiler von $n^2 + 23$.
3. Man zeige: Ist $n > 1$, und ist $a^n - 1$ eine Primzahl, so müssen $a = 2$ und n eine Primzahl sein.
4. Unter Benutzung der Identität $47 = 2^7 - 3^4$ weise man nach, daß 47 ein Teiler von $2^{23} - 1$ ist.
5. Man zeige: Ist $a \geqq 2$, und ist $a^n + 1$ eine Primzahl, so ist a gerade und n eine Potenz von 2.
6. Man weise nach, daß die Zahlen $2^{2^n} + 1$ ($n = 0, 1, 2, \ldots$) paarweise teilerfremd sind und leite daraus einen neuen Beweis für den Satz 1.2 ab. — G. Pólya.
7. Sind a, b, n drei natürliche Zahlen, so beweise man

   $$(n^a - 1, n^b - 1) = n^{(a,b)} - 1$$

   durch Anwendung des Euklidischen Algorithmus.

8. Man zeige: Sind a, b, c, d natürliche Zahlen, die der Bedingung $ab = cd$ genügen, so ist

$$a = \frac{(a, c)\ (a, d)}{(a, b, c, d)}.$$

— Lauffer.

9. Es seien n, n_1, n_2 natürliche Zahlen mit $n \mid n_1 n_2$, $n \nmid n_1$, $n \nmid n_2$. Man zeige, daß dann

$$d = \frac{n_1}{\left(n_1, \frac{n_1 n_2}{n}\right)}$$

ein Teiler von n mit $1 < d < n$ ist. — W. Sierpiński.

10. Es sei $n = a^2 + b^2 = c^2 + d^2$ mit natürlichen Zahlen a, b, c, d, die den Bedingungen $a \geqq b$, $c \geqq d$, $a > c$, $(a, b) = (c, d) = 1$ unterliegen. Dann ist

$$t = \frac{ac + bd}{(ac + bd,\ ab + cd)}$$

ein Teiler von n mit $1 < t < n$. — W. Sierpiński.

11. Ein Polynom $P(x)$ mit reellen Koeffizienten heißt *ganzwertig*, wenn $P(n)$ ganzzahlig für beliebige ganze Zahlen n ausfällt. Es ist nachzuweisen, daß ein solches Polynom auf genau eine Weise in der Form

$$P(x) = a_0 + a_1 \binom{x}{1} + a_2 \binom{x}{2} + \cdots + a_n \binom{x}{n}$$

mit ganzzahligen Koeffizienten darstellbar ist.

12. Es sei $P(x)$ ein ganzwertiges Polynom. Man zeige, daß nicht alle Glieder der Zahlenfolge $P(0), P(1), P(2), \ldots$ Primzahlen sein können.
Man betrachte insbesondere das Beispiel

$$P(x) = 2 \binom{x}{2} + 41.$$

Anleitung: Im Sinne eines indirekten Beweises untersuche man $P(0) = p$ und gebe eine natürliche Zahl x so an, daß $P(x) > p$ und $p \mid P(x)$ wird.

2. Kongruenzen

In diesem Kapitel soll die elementare Teilbarkeitslehre weiter ausgebaut werden. Wir betrachten solche ganzen Zahlen a, b, die bei der Teilung durch die natürliche Zahl m denselben Rest r lassen: Es sei $a = k_1 m + r$, $b = k_2 m + r$ mit ganzen Zahlen k_1, k_2, r und etwa $0 \leqq r < m$. Welche gemeinsamen Eigenschaften haben a, b hinsichtlich m? Zunächst ist

$$a - b = (k_1 - k_2)\, m = qm$$

oder

$$a = b + qm\,.$$

Also ist $m \mid (a - b)$. Ist ferner t ein Teiler von a und m, so auch von b. Entsprechend ist jeder Teiler d von b und m auch ein Teiler von a. Noch schärfer überblickt man sofort $(a, m) = (b, m)$. Diese Eigenschaften erweisen sich als so grundlegend, daß eine formale Festlegung des Begriffes der Restgleichheit äußerst zweckmäßig erscheint. Dem Studium der Grundlagen der Theorie der Kongruenzen, das heißt der Restgleichheit, die von C. F. Gauss (1777—1855) erstmals entwickelt wurde, ist dieses Kapitel gewidmet.

2.1. Der Restklassenring

Definition 2.1. Gegeben seien die ganzen Zahlen a, b, m mit $m > 0$. a heiße *kongruent b modulo m*, in Zeichen $a \equiv b \pmod{m}$, wenn m ein Teiler der Differenz $a - b$ ist.

Ist a nicht zu b modulo m kongruent, so nennen wir a, b *inkongruent* und schreiben $a \not\equiv b \pmod{m}$.

Die *Kongruenzrelation* R_m nach dem Modul m bildet in $\mathbf{Z}$ offenbar eine *Äquivalenzrelation*. Denn aus der Definition ergeben sich unmittelbar

$$a \equiv a \pmod{m} \quad \text{(Reflexivität)},$$

$$a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m} \quad \text{(Symmetrie)},$$

$$a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m} \quad \text{(Transitivität)}.$$

Demzufolge bewirkt R_m im Ring $\mathbf{Z}$ eine Klasseneinteilung $\mathbf{Z}/R_m$.

Definition 2.2. Gegeben sei ein fester Modul $m > 0$. Mit $\bar{a}$ werde die Menge aller ganzen Zahlen x mit $x \equiv a \pmod{m}$ bezeichnet. Die Menge $\bar{a}$ heiße dann *Restklasse* modulo m.

Die Restklasse

$$\bar{a} = \{x : x \in \mathbf{Z}, x \equiv a \pmod{m}\}$$

enthält also alle diejenigen ganzen Zahlen x, die hinsichtlich der Teilung durch m denselben Rest a lassen. Damit gilt

$$\bar{a} = \bar{b} \Leftrightarrow a \equiv b \pmod{m},$$

und die Menge $\mathbf{Z}/R_m$ besteht aus allen Restklassen modulo m. Die Anzahl ihrer Elemente ist natürlich m.

Definition 2.3. Wir sagen, die Zahlen $a_1, a_2, \ldots, a_m$ bilden ein *vollständiges Restsystem* modulo m, wenn für $i \neq j$ stets $a_i \not\equiv a_j \pmod{m}$ gilt.

Beispielsweise bilden die Zahlen $0, 1, \ldots, m-1$ ein vollständiges Restsystem modulo m, und wir können die Menge der Restklassen etwa durch

$$\mathbf{Z}/R_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$$

beschreiben.

Das Rechnen mit Kongruenzen ist überaus einfach. Ist

$$a_1 \equiv b_1 \pmod{m}, \quad a_2 \equiv b_2 \pmod{m},$$

also

$$a_1 = b_1 + k_1 m, \quad a_2 = b_2 + k_2 m,$$

so ergibt Addition beziehungsweise Multiplikation der Gleichungen

$$a_1 + a_2 = b_1 + b_2 + (k_1 + k_2)\, m,$$
$$a_1 \cdot a_2 = b_1 \cdot b_2 + (b_1 k_2 + b_2 k_1 + m\, k_1 k_2)\, m.$$

Hieraus folgt

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{m}, \qquad a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}.$$

Dies rechtfertigt die folgende Definition für das Rechnen mit Restklassen:

Definition 2.4. $\bar{a} + \bar{b} = \overline{a+b}, \qquad \bar{a} \cdot \bar{b} = \overline{ab}.$

Die oben angeführten Rechnungen zeigen zugleich, daß diese Definitionen der Rechenoperationen in $\mathbf{Z}/R_m$ unabhängig von der Auswahl der Repräsentanten in den Restklassen ist. Allgemein kann man sagen, daß das Rechnen mit Restklassen auf das Rechnen mit ganzen Zahlen zurückgeführt ist. Präziser heißt das:

Satz 2.1. *Die Menge der Restklassen* $\mathbf{Z}/R_m$ *bildet hinsichtlich der in Definition* 2.4 *ausgesprochenen algebraischen Operationen einen kommutativen Ring.*

Ein ins Detail gehender Beweis erübrigt sich wohl. In $\mathbf{Z}/R_m$ bilden $\bar{0}$ das Nullelement und $\bar{1}$ das Einselement.

Wir stellen jetzt die Frage nach der *Division im Restklassenring*. Ist der Modul m eine zusammengesetzte Zahl $m = m_1 m_2$ mit $1 < m_1 < m$, so ist sowohl $\overline{m}_1 \neq \bar{0}$ als

auch $\overline{m}_2 \neq \bar{0}$. Aber für das Produkt der Restklassen finden wir $\overline{m}_1 \cdot \overline{m}_2 = \overline{m_1 m_2} = \bar{0}$, so daß der Ring Nullteiler enthält. Eine andere Situation finden wir vor, wenn der Modul $m = p$ eine Primzahl ist. Ist $\bar{a} \cdot \bar{b} = \bar{0}$ in $\mathbf{Z}/R_p$ so bedeutet dies $p \mid ab$, also $p \mid a$ oder $p \mid b$, das heißt $\bar{a} = \bar{0}$ oder $b = \bar{0}$. Demnach enthält $\mathbf{Z}/R_p$ keine Nullteiler und ist folglich ein Integritätsbereich. Aus der Algebra ist bekannt, daß ein endlicher Integritätsbereich automatisch einen Körper darstellt. Da für alle $\bar{a} \in \mathbf{Z}/R_p$ gilt $p\bar{a} = \overline{pa} = \bar{0}$, so sagt man auch, es handelt sich um einen Körper der Charakteristik p. Zusammenfassend halten wir fest:

Satz 2.2. *Der Restklassenring $\mathbf{Z}/R_m$ besitzt für zusammengesetztes m Nullteiler. Ist $m = p$ eine Primzahl, so ist er ein Körper der Charakteristik p.*

Die Frage der Lösbarkeit der Gleichung $\bar{a}\bar{x} = \bar{b}$ bei vorgegebenen $\bar{a}$, $\bar{b}$, mit $\bar{a} \neq \bar{0}$ ist nach diesem Satz in $\mathbf{Z}/R_p$ entschieden. Sie soll aber auch in beliebigen Ringen $\mathbf{Z}/R_m$ behandelt werden. Eine äquivalente Formulierung des Problems besteht in der Frage nach der Lösbarkeit der linearen Kongruenz $ax \equiv b \pmod{m}$. In diesem Sinne sprechen wir den folgenden Satz aus:

Satz 2.3. *Die Kongruenz*

$$ax \equiv b \pmod{m}$$

ist genau dann lösbar, wenn $(a, m) \mid b$. In diesem Fall besitzt sie genau (a, m) zueinander modulo m inkongruente Lösungen.

Beweis. Die genannte Bedingung ist notwendig, denn andernfalls kann eine Gleichung $ax = b + km$ in ganzen Zahlen nicht bestehen. Es sei also jetzt $(a, m) = d$ und $d \mid b$.

1. Fall: $d = 1$. Nach Satz 1.4 gibt es ganze Zahlen u, v mit

$$au + mv = 1.$$

Also gibt es auch ganze Zahlen x, y mit

$$ax + my = b,$$

was

$$ax \equiv b \pmod{m}$$

zur Folge hat. Die Lösung ist in dem Sinne eindeutig bestimmt, daß alle x und x' mit

$$ax \equiv b \pmod{m}, \qquad ax' \equiv b \pmod{m}$$

zur selben Restklasse gehören. Denn aus diesen beiden Kongruenzen folgt

$$a(x - x') \equiv 0 \pmod{m}$$

und wegen $d = 1$

$$x \equiv x' \pmod{m}.$$

2. Fall: $d > 1$. Als notwendig für die Lösbarkeit wurde bereits $d \mid b$ erkannt. Setzt man in

$$ax = b + km$$

$a = a'd$, $b = b'd$, $m = m'd$, so ist nach Teilung durch d

$$a'x \equiv b' \quad (m').$$

Nach Fall 1 besitzt diese Kongruenz eine eindeutig bestimmte Lösungsklasse

$$x \equiv x_0 \quad (m').$$

Modulo m ergeben sich hieraus die d Lösungen

$$x \equiv x_0, x_0 + m', \ldots, x_0 + (d-1)\, m' \quad (m).$$

2.2. Die prime Restklassengruppe

Die Aussage des Satzes 2.3, daß $\bar{a} \cdot \bar{x} = \bar{b}$ in $\mathbf{Z}/R_m$ für $(a, m) = 1$ eine eindeutig bestimmte Lösung hat, gibt uns Veranlassung, diese Restklassen $\bar{a}$ näher zu betrachten.

Definition 2.5. Die Restklasse $\bar{a}$ heißt eine *prime Restklasse* modulo m, wenn $(a, m) = 1$ gilt.

Satz 2.4. *Die primen Restklassen modulo m bilden eine multiplikative abelsche Gruppe, die prime Restklassengruppe modulo m.*

Beweis. Es bezeichne G die Menge der primen Restklassen. Die Gruppenaxiome überprüft man leicht:

1. $\bar{a}, \bar{b} \in G \Rightarrow (a, m) = (b, m) = 1 \Rightarrow (ab, m) = 1 \Rightarrow \bar{a}\bar{b} = \overline{ab} \in G$.
2. Kommutativ- und Assoziativgesetz sind erfüllt.
3. Das Einselement ist $\bar{1}$.
4. Nach Satz 2.3 existiert zu jedem Element genau ein Inverses.

Definition 2.6. Es bezeichne $\varphi(m)$ die *Anzahl der primen Restklassen modulo m.*

$\varphi(m)$ ist damit eine Funktion von m, wenn sie auch nur für natürliche Zahlen m erklärt ist. In einem solchen Fall spricht man von einer *zahlentheoretischen Funktion.* $\varphi(m)$ wird nach L. Euler (1707—1783), der sie in die Zahlentheorie einführte, auch als *Eulersche φ-Funktion* bezeichnet. Entsprechend der Definition kann man auch sagen, $\varphi(m)$ gibt die *Anzahl der zu m teilerfremden natürlichen Zahlen an*, die kleiner oder gleich m sind. Die ersten Werte von $\varphi(m)$ sind: $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$. Ist $m = p$ eine Primzahl, so ist offensichtlich $\varphi(p) = p - 1$. Die folgenden Sätze dienen der Berechnung der Eulerschen φ-Funktion.

Satz 2.5.

$$\sum_{t \mid n} \varphi(t) = n.$$

Die Summe ist über alle Teiler t von n zu erstrecken.

Beweis. Es bezeichne $\varphi_d(n)$ die Anzahl der natürlichen Zahlen $x \leqq n$ mit $(x, n) = d$. Dann ist

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

Setzt man $x = x'd$, $n = n'd$, so ist $\varphi_d(n) = \varphi(n')$ wegen $(x', n') = 1$. Mit $n' = \frac{n}{d}$ ist

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

Mit Hilfe dieses Satzes läßt sich leicht $\varphi(n)$ für eine Primzahlpotenz $n = p^\nu$ ($\nu \geqq 1$) berechnen. Es ist

$$\varphi(1) + \varphi(p) + \cdots + \varphi(p^{\nu-1}) + \varphi(p^\nu) = p^\nu,$$
$$\varphi(1) + \varphi(p) + \cdots + \varphi(p^{\nu-1}) = p^{\nu-1}.$$

Durch Subtraktion der Gleichungen folgt

$$\varphi(p^\nu) = p^\nu\left(1 - \frac{1}{p}\right). \tag{1}$$

Hilfssatz 2.1. *Es seien m, m' zwei natürliche Zahlen mit $(m, m') = 1$. Durchlaufen a und a' ein vollständiges Restsystem modulo m bzw. modulo m', dann durchläuft $a'm + am'$ ein vollständiges Restsystem modulo mm'.*

Beweis: Die Anzahl der Zahlen $a'm + am'$ ist offensichtlich mm'. Aus

$$a_1'm + a_1m' \equiv a_2'm + a_2m' \quad (mm')$$

folgt

$$a_1m' \equiv a_2m' \quad (m),$$
$$a_1'm \equiv a_2'm \quad (m'),$$

also wegen $(m, m') = 1$

$$a_1 \equiv a_2 \quad (m), \qquad a_1' \equiv a_2' \quad (m').$$

Daher sind alle Zahlen $a'm + am'$ untereinander inkongruent.

Satz 2.6. $(m, m') = 1 \Rightarrow \varphi(mm') = \varphi(m)\,\varphi(m')$.

Beweis. Nach dem Hilfssatz durchläuft $a'm + am'$ unter der Voraussetzung $(m, m') = 1$ ein vollständiges Restsystem modulo mm', wenn a und a' ein solches modulo m beziehungsweise m' durchlaufen. Dabei ist

$$(a'm + am', mm') = 1 \Leftrightarrow (a'm + am', m) = 1 \wedge (a'm + am', m') = 1$$
$$\Leftrightarrow (am', m) = 1 \wedge (a'm, m') = 1$$
$$\Leftrightarrow (a, m) = 1 \wedge (a', m') = 1.$$

Damit sind die $\varphi(mm')$ zu mm' teilerfremden Zahlen unterhalb mm' die kleinsten

positiven Reste der $\varphi(m)$ $\varphi(m')$ Zahlen $a'm + am'$ mit $(a, m) = 1$ und $(a', m') = 1$. Das ist die Behauptung.

Satz 2.7.

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

Das Produkt ist dabei über alle Primteiler von m zu erstrecken.

Beweis. Wir betrachten die kanonische Zerlegung von m

$$m = \prod_{i=1}^{r} p_i^{\nu_i}, \qquad p_i \neq p_j \quad \text{für} \quad i \neq j.$$

Nach Satz 2.6 und (1) ist

$$\varphi(m) = \prod_{i=1}^{r} \varphi(p_i^{\nu_i}) = \prod_{i=1}^{r} p_i^{\nu_i} \left(1 - \frac{1}{p_i}\right) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right).$$

Die Eulersche φ-Funktion ist von wesentlicher Bedeutung in der Zahlentheorie, wie schon der nächste Satz lehrt. P. DE FERMAT (1601—1665) bemerkte, daß

$$a^{p-1} \equiv 1 \quad (p)$$

für Primzahlen p mit $p \nmid a$ gilt, was gelegentlich als *kleiner Fermatscher Satz* angesprochen wird. Der folgende Satz gibt eine von L. EULER ausgesprochene Verallgemeinerung dieser Aussage.

Satz 2.8 (FERMAT-EULER).

$$(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \quad (m).$$

Beweis. Wir betrachten die prime Restklassengruppe modulo m

$$G = \{\bar{a}_1, \bar{a}_2, \ldots, \overline{a_{\varphi(m)}}\}.$$

Es sei $\bar{a} \in G$, dann ist

$$G = \{\overline{aa_1}, \overline{aa_2}, \ldots, \overline{aa_{\varphi(m)}}\}$$

wieder die volle prime Restklassengruppe. Daher ist

$$\overline{aa_1} \cdot \overline{aa_2} \cdot \ldots \cdot \overline{aa_{\varphi(m)}} = \bar{a}_1 \bar{a}_2 \cdot \ldots \cdot \overline{a_{\varphi(m)}},$$

also

$$\overline{a^{\varphi(m)}} = \bar{1}.$$

Das Beispiel $2^3 \equiv 1$ (7) lehrt, daß $\varphi(m)$ nicht der kleinste Exponent sein muß, so daß eine Potenz von a den Rest 1 modulo m läßt. Ist aber d die kleinste natürliche Zahl mit

$$a^d \equiv 1 \quad (m), \qquad (a, m) = 1,$$

so ist $d \mid \varphi(m)$. Denn sei $\varphi(m) = kd + r$ mit $0 \leqq r < d$, so ist

$$1 \equiv a^{\varphi(m)} \equiv a^{kd+r} \equiv a^r \quad (m),$$

und wegen der Minimaleigenschaft von d muß $r = 0$ sein.

Der Satz von FERMAT-EULER ermöglicht eine unmittelbare *Auflösung der linearen Kongruenz*

$$ax \equiv b \quad (m), \qquad (a, m) = 1.$$

Aus

$$ax \equiv ba^{\varphi(m)} \quad (m)$$

ergibt sich wegen $(a, m) = 1$

$$x \equiv ba^{\varphi(m)-1} \quad (m). \tag{2}$$

Jedoch hat dieses Ergebnis mehr theoretisches als praktisches Interesse, denn die Berechnung der Potenz $a^{\varphi(m)}$ kann recht mühsam sein.

Satz 2.9 (WILSON). *Für jede Primzahl p gilt*

$$(p-1)! \equiv -1 \quad (p).$$

Beweis. Für $p = 2$ ist die Behauptung sicher richtig. Für $p > 2$ betrachten wir die prime Restklassengruppe

$$G = \{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}.$$

In G ist die Gleichung $\bar{a}\bar{x} = \bar{1}$ eindeutig nach $\bar{x}$ auflösbar. Wann ist $\bar{x} = \bar{a}$?

$$\bar{a}^2 = \bar{1} \Leftrightarrow a^2 \equiv 1 \quad (p) \Leftrightarrow (a-1)(a+1) \equiv 0 \quad (p)$$
$$\Leftrightarrow \bar{a} = \bar{1} \vee \bar{a} = \overline{p-1}.$$

Damit können wir in dem Produkt

$$\overline{(p-1)}! = \bar{1} \cdot \bar{2} \cdot \ldots \cdot \overline{p-1}$$

die Restklassen außer $\bar{1}, \overline{p-1}$ zu Paaren zusammenfügen mit $\bar{a}\bar{b} = \bar{1}$. Also ist

$$\overline{(p-1)}! = \overline{p-1},$$

und das ist die Behauptung des Satzes.

Der Satz von WILSON ist ein *Primzahlkriterium*, das heißt, aus

$$(n-1)! \equiv -1 \quad (n) \qquad (n > 1)$$

folgt, daß $n = p$ eine Primzahl sein muß. Ist nämlich n eine zusammengesetzte Zahl, so gibt es eine Zahl d mit $d \mid n$ und $1 < d < n$. Dann ist aber auch $d \mid (n-1)!$.

2.3. Lineare diophantische Gleichungen

In Anwendung des Rechnens mit Kongruenzen sollen jetzt lineare Gleichungen

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c \tag{3}$$

mit ganzzahligen Koeffizienten $a_1, a_2, \ldots, a_n, c$ behandelt werden. Dabei sollen die ganzzahligen Lösungen $x_1, x_2, \ldots, x_n$ — sofern vorhanden — dieser Gleichung bestimmt werden. Die Bezeichnung „diophantisch" ist dem Namen des Mathematikers DIOPHANT (um 250) entlehnt und zeigt allgemein an, daß man ausschließlich an ganzzahligen Lösungen einer Gleichung interessiert ist.

Wir befassen uns zunächst mit der Gleichung

$$ax + by = c; \qquad a, b, c \in \mathbf{Z}; \qquad a, b \neq 0. \tag{4}$$

Bekanntlich beschreibt diese Gleichung in der Euklidischen Ebene bei beliebigen reellen x, y eine Gerade. Wir nennen nun solche Punkte P mit den Koordinaten x, y der Ebene *Gitterpunkte*, deren Koordinaten beide ganzzahlig sind. Somit kann unser arithmetisches Problem auch geometrisch beschrieben werden: Liegen auf der durch (4) beschriebenen Geraden Gitterpunkte und, wenn ja, welche? Man überblickt sofort, daß $(a, b) \mid c$ notwendige Bedingung für die Lösbarkeit der Gleichung (4) in ganzen Zahlen ist. Da man den größten gemeinsamen Teiler dann wegkürzen kann, beschränken wir uns auf den Fall $(a, b) = 1$. Es wird sich zeigen, daß unter dieser Voraussetzung die Gleichung (4) lösbar ist, und wir werden die Lösungen angeben. Betrachten wir (4) modulo $|b|$, so folgt aus

$$ax \equiv c \quad (|b|)$$

und wegen $(a, b) = 1$

$$x \equiv ca^{\varphi(|b|)-1} \quad (|b|)$$

und mit beliebiger ganzer Zahl k

$$x = ca^{\varphi(|b|)-1} + kb. \tag{5}$$

Setzt man (5) in (4) ein, so errechnet sich y zu

$$y = c\,\frac{1 - a^{\varphi(|b|)}}{b} - ka. \tag{6}$$

y ist nach dem Satz von FERMAT-EULER tatsächlich ganzzahlig, so daß (5) und (6) die Lösungen von (4) unter der Voraussetzung $(a, b) = 1$ darstellen.

Lineare diophantische Gleichungen mit n Unbekannten können nach dem geschilderten Verfahren auf solche mit $n - 1$ Unbekannten zurückgeführt werden. Es bezeichne $d_k = (a_1, a_2, \ldots, a_k)$ für $k = 2, 3, \ldots, n$. Wir betrachten die Gleichung (3) gleich unter der Voraussetzung $d_n = 1$. Schreiben wir die Gleichung in der Gestalt

$$a_1x_1 + a_2x_2 + \cdots + a_{n-1}x_{n-1} = c - a_nx_n,$$

so erkennt man, daß notwendigerweise

$$a_n x_n \equiv c \pmod{d_{n-1}}$$

sein muß. Wegen $(a_n, d_{n-1}) = d_n = 1$ ist diese Kongruenz eindeutig lösbar, und mit beliebiger ganzer Zahl k ist

$$x_n = c a_n^{\varphi(d_{n-1})-1} + k d_{n-1}.$$

Damit ist Gleichung (3) mit n Unbekannten auf die Gleichung

$$a_1 x_1 + a_2 x_2 + \cdots + a_{n-1} x_{n-1} = c(1 - a_n^{\varphi(d_{n-1})}) - k a_n d_{n-1}$$

mit $n - 1$ Unbekannten zurückgeführt.

2.4. Simultane lineare Kongruenzen

Ein System von linearen Kongruenzen muß keine gemeinsame Lösung besitzen, auch wenn die einzelnen Kongruenzen Lösungen haben. Zum Beispiel hat das System von Kongruenzen $x \equiv 0 \pmod 2$, $x \equiv 1 \pmod 4$ offensichtlich keine gemeinsame Lösung. Man bemerkt an diesem Beispiel $(2,4) > 1$. Sind dagegen die Moduln teilerfremd, so liegt eine besondere Situation vor.

Satz 2.10. *Die Zahlen $m_1, m_2, \ldots, m_r$ seien paarweise teilerfremd. $a_1, a_2, \ldots, a_r$ und $b_1, b_2, \ldots, b_r$ seien beliebige ganze Zahlen mit $(a_1, m_1) = (a_2, m_2) = \cdots = (a_r, m_r) = 1$. Dann besitzt das System*

$$a_i x \equiv b_i \pmod{m_i} \qquad (i = 1, 2, \ldots, r)$$

genau eine Lösung modulo $m = m_1 m_2 \cdot \cdots \cdot m_r$.

Beweis. Nach Satz 2.3 besitzen die einzelnen Kongruenzen genau eine Lösung. Notieren wir sie uns etwa in der Form

$$x_i \equiv c_i \pmod{m_i} \qquad (i = 1, 2, \ldots, r).$$

Wegen $(m_i, m_j) = 1$ für $i \neq j$ ist $\left(\frac{m}{m_1}, \frac{m}{m_2}, \ldots, \frac{m}{m_r}\right) = 1$. Nach Satz 1.4 gibt es ganze Zahlen $y_1, y_2, \ldots, y_r$ mit

$$\frac{m}{m_1} y_1 + \frac{m}{m_2} y_2 + \cdots + \frac{m}{m_r} y_r = 1.$$

Wir können uns ganze Zahlen $e_1, e_2, \ldots, e_r$ wählen mit

$$e_i \equiv \frac{m}{m_i} y_i \pmod{m} \qquad (i = 1, 2, \ldots, r),$$

etwa die absolut kleinsten Reste modulo m oder auch die erwähnten Zahlen selbst.

Jedenfalls gilt

$$e_1 + e_2 + \cdots + e_r \equiv 1 \quad (m), \tag{7}$$

$$e_i e_j \equiv 0 \quad (m) \qquad (i \neq j), \qquad e_i e_i \equiv e_i \quad (m), \tag{8}$$

$$e_j \equiv \begin{cases} 0 & (m_i) \quad \text{für} \quad i \neq j \\ 1 & (m_i) \quad \text{für} \quad i = j. \end{cases} \tag{9}$$

Bilden wir

$$x_0 = c_1 e_1 + c_2 e_2 + \cdots + c_r e_r,$$

so ist wegen (9)

$$x_0 \equiv c_i \quad (m_i) \qquad (i = 1, 2, \ldots, r)$$

und daher $x \equiv x_0 \quad (m)$ eine gemeinsame Lösung des Systems. Für jede andere Lösung x_0' modulo m ist

$$x_0' \equiv x_0 \quad (m_i) \qquad (i = 1, 2, \ldots, r)$$

und folglich auch $x_0' \equiv x_0 \quad (m)$. Damit ist der Satz vollständig bewiesen.

Die Bedeutung dieses Satzes werden wir im nachfolgenden Abschnitt erkennen.

2.5. Die Struktur der primen Restklassengruppe

Es bezeichne G_m die prime Restklassengruppe modulo m. Sie ist eine endliche abelsche Gruppe der Ordnung $\varphi(m)$. Die Untersuchung ihrer algebraischen Struktur wird uns zu tieferen zahlentheoretischen Einsichten führen.

Für m bestehe mit paarweisen teilerfremden Zahlen $m_1, m_2, \ldots, m_r$ die Zerlegung $m = m_1 m_2 \cdot \cdots \cdot m_r$. Nach Satz 2.10 besitzt das System von Kongruenzen

$$x \equiv a_i \quad (m_i) \qquad (i = 1, 2, \ldots, r)$$

genau eine Lösung $x \equiv a \quad (m)$. Dabei ist $(a, m_i) = (a_i, m_i)$ für $i = 1, 2, \ldots, r$. Also ist $\bar{a}$ genau dann eine prime Restklasse modulo m, wenn die $\bar{a}_i$ prime Restklassen modulo m_i sind. Nach Satz 2.10 gestattet demnach jede prime Restklasse $\bar{a}$ mit den durch (7)—(9) definierten Zahlen e_i die eindeutig bestimmte Zerlegung

$$\bar{a} = \overline{a_1 e_1} + \overline{a_2 e_2} + \cdots + \overline{a_r e_r}. \tag{10}$$

Bezeichnet $\bar{a}_i^* \in G_m$ die prime Restklasse

$$\bar{a}_i^* := \overline{e_1 + \cdots + e_{i-1} + a_i e_i + e_{i+1} + \cdots + e_r},$$

so bildet offensichtlich bei festem i die Menge $G_{m_i}^*$ der Restklassen $\bar{a}_i^*$ eine Untergruppe von G_m. Weiter erhält man aus (10) auf Grund der Eigenschaften (7)—(9) die eindeutig bestimmte Zerlegung

$$\bar{a} = \bar{a}_1^* \bar{a}_2^* \cdot \cdots \cdot \bar{a}_r^*.$$

Führt man diese Zerlegung für alle $\bar{a} \in G_m$ durch, so heißt das in der Sprache der Algebra (vgl. MfL, Bd. 3): *Die prime Restklassengruppe G_m ist das direkte Produkt der Untergruppen $G^*_{m_1}, G^*_{m_2}, \ldots, G^*_{m_r}$.* Ferner läßt sich die Gruppe $G^*_{m_i}$ auf die prime Restklassengruppe G_{m_i} mit Hilfe der Zuordnung $\bar{a}_i^* \leftrightarrow \bar{a}_i$ isomorph abbilden. Damit haben wir:

Satz 2.11. *Ist $m = m_1 \cdot m_2 \cdot \cdots \cdot m_r$ mit paarweise teilerfremden Zahlen m_i, so ist die prime Restklassengruppe modulo m isomorph dem direkten Produkt der primen Restklassengruppen modulo m_i.*

Nimmt man für m die kanonische Zerlegung nach Primzahlpotenzen, so besagt dieser Satz, daß die prime Restklassengruppe modulo m beherrscht wird, sofern wir Kenntnis über die primen Restklassengruppen modulo einer Primzahlpotenz besitzen. Bevor wir uns diesen Gruppen zuwenden, führen wir noch den Begriff der *primitiven Wurzel* ein, der im engen Zusammenhang damit steht.

Nach dem Satz von Fermat-Euler gibt es zu zwei ganzen Zahlen a, m mit $m > 1$, $(a, m) = 1$ stets eine natürliche Zahl d mit $a^d \equiv 1 \pmod{m}$. Dabei ist $d \mid \varphi(m)$. Die Beispiele $7^6 \equiv 1 \pmod{43}$ und $5^n \not\equiv 1 \pmod{7}$ für $1 \leq n < 6$ zeigen, daß beide Möglichkeiten $d < \varphi(m)$ und $d = \varphi(m)$ auftreten können. Wir führen die Sprechweise ein:

a gehört modulo m zum Exponenten d, wenn $a^d \equiv 1 \pmod{m}$ ist,
aber $a^n \not\equiv 1 \pmod{m}$ für $1 \leq n < d$.

Hilfssatz 2.2. *Gehört a modulo m zum Exponenten d, so sind die Zahlen $1, a, a^2, \ldots, a^{d-1}$ modulo m inkongruent. Ist ferner $a^t \equiv 1 \pmod{m}$, so ist $d \mid t$.*

Beweis. Es sei $0 \leq h < k < d$ und $a^k \equiv a^h \pmod{m}$. Wegen $(a, m) = 1$ ist dann $a^{k-h} \equiv 1 \pmod{m}$. Und dies steht infolge $0 < k - h < d$ im Widerspruch zur Auswahl von d als kleinstem Exponenten. Nimmt man t in der Form $t = dq + r$ mit $0 \leq r < d$, so zeigt

$$1 \equiv a^t \equiv a^{dq+r} \equiv a^r \pmod{m},$$

daß $r = 0$ sein muß.

Hilfssatz 2.3. *Gehört a modulo m zum Exponenten d, und ist n eine natürliche Zahl mit $(n, d) = 1$, so gehört a^n ebenfalls zum Exponenten d.*

Beweis. a^n gehöre zum Exponenten t. Aus $(a^n)^t \equiv 1 \pmod{m}$ und Hilfssatz 2.2 folgt $d \mid nt$. Da $(n, d) = 1$ vorausgesetzt ist, gilt sogar $d \mid t$ und schwächer $d \leq t$. Da $(a^n)^d = (a^d)^n \equiv 1 \pmod{m}$ ist, kann andererseits nur $d \geq t$ sein. Insgesamt ist also $t = d$.

Definition 2.7. Eine Zahl g, die modulo m zum Exponenten $\varphi(m)$ gehört, heißt *primitive Wurzel* modulo m.

Die bereits erwähnten Beispiele besagen also: 5 ist primitive Wurzel modulo 7. Dagegen gehört 7 modulo 43 zum Exponenten 6 und ist keine primitive Wurzel.

Satz 2.12. *Zu einem Modul m gibt es entweder keine oder $\varphi\big(\varphi(m)\big)$ modulo m inkongruente primitive Wurzeln.*

Beweis. Es sei g primitive Wurzel modulo m. Nach Hilfssatz 2.3 ist auch g^n primitive Wurzel modulo m, sofern $(n, \varphi(m)) = 1$ gibt. Es gibt $\varphi(\varphi(m))$ derartige Zahlen $n \leqq \varphi(m)$. Also gibt es jedenfalls $\varphi(\varphi(m))$ primitive Wurzeln. Daß es keine weiteren primitiven Wurzeln gibt, zeigt der Hilfssatz 2.2. Durchläuft nämlich ν die Zahlen von 0 bis $\varphi(m) - 1$, so durchläuft g^ν das prime Restsystem modulo m. Ist ν so gewählt, daß $(\nu, \varphi(m)) = t > 1$, dann ist $(g^\nu)^{\frac{\varphi(m)}{t}} \equiv 1 \pmod{m}$. Also kann g^ν nicht primitive Wurzel sein.

Die Aufgabe, alle Moduln m zu bestimmen, zu denen primitive Wurzeln existieren, hängt wesentlich mit der Struktur der primen Restklassengruppe modulo m zusammen, wie sich in folgendem zeigen wird.

Satz 2.13. *Es sei p eine Primzahl. Die prime Restklassengruppe modulo p ist zyklisch. Mit anderen Worten: Es gibt primitive Wurzeln modulo p.*

Ist also g eine primitive Wurzel modulo p, so läßt sich jede prime Restklasse $\bar{a}$ durch $\bar{a} = \overline{g^n}$ mit $0 \leqq n \leqq p - 1$ darstellen.

Beweis. Für $p = 2$ ist die Aussage des Satzes trivial. Es sei jetzt p eine ungerade Primzahl. Für $d \mid (p - 1)$ erklären wir $\chi(d)$ als die Anzahl der Restklassen, die zum Exponenten d gehören. Wir haben also $\chi(p - 1) > 0$ zu zeigen. Nach Satz 2.12 ist dann sogar $\chi(p - 1) = \varphi(p - 1)$.

Gibt es eine Zahl a, die zum Exponenten d gehört, so sind nach Hilfssatz 2.2 die sämtlichen Zahlen $1, a, a^2, \ldots, a^{d-1}$ inkongruente Lösungen von $x^d - 1 \equiv 0 \pmod{p}$. Demzufolge läßt sich die Polynomkongruenz in der Gestalt

$$x^d - 1 \equiv (x - 1)(x - a) \cdot \cdots \cdot (x - a^{d-1}) \equiv 0 \pmod{p}$$

schreiben. Also sind die genannten Zahlen auch sämtliche Lösungen dieser Kongruenz. Nach Hilfssatz 2.3 gehört mit a auch a^k zum Exponenten d, wenn $(k, d) = 1$. Das heißt, unter den Lösungen befinden sich $\varphi(d)$ Zahlen, die zum Exponenten d gehören. Zusammenfassend ist entweder $\chi(d) = 0$ oder $\chi(d) = \varphi(d)$.

Die Aufzählung aller primen Restklassen nach ihren zugehörigen Exponenten geordnet ergibt

$$\sum_{d \mid (p-1)} \chi(d) = p - 1.$$

Da nach Satz 2.5 aber auch

$$\sum_{d \mid (p-1)} \varphi(d) = p - 1$$

gilt, kann nur $\chi(d) = \varphi(d)$ für alle d sein. Damit ist der Satz bewiesen.

Der Untersuchung der primen Restklassengruppe modulo p^ν ($\nu > 1$) schicken wir zwei Hilfssätze voraus.

Hilfssatz 2.4. *Es gibt eine primitive Wurzel g modulo p mit der Eigenschaft*

$$g^{p-1} \not\equiv 1 \pmod{p^2}.$$

Beweis. Erfüllt die primitive Wurzel g diese Eigenschaft nicht, so muß $g^{p-1} \equiv 1$ (p^2) sein. Dann betrachten wir die primitive Wurzel $g_1 = g + p$. Für sie gilt

$$\begin{aligned} g_1^{p-1} &= (g+p)^{p-1} \equiv g^{p-1} + (p-1)\, g^{p-2} p \quad (p^2) \\ &\equiv 1 - p g^{p-2} \quad (p^2) \\ &\not\equiv 1 \quad (p^2), \end{aligned}$$

also die geforderte Eigenschaft.

Hilfssatz 2.5. *Ist g eine primitive Wurzel modulo p $(p > 2)$ mit*

$$g^{p-1} \not\equiv 1 \quad (p^2),$$

so gilt für jedes $r \geqq 2$

$$g^{\varphi(p^{r-1})} \not\equiv 1 \quad (p^r). \tag{11}$$

Beweis. Wir führen den Bereis durch Induktion nach r. Für $r = 2$ ist (11) nach Voraussetzung richtig. Wir nehmen die Richtigkeit von (11) für ein $r \geqq 2$ an. Nach dem Satz von FERMAT-EULER ist

$$\begin{aligned} g^{\varphi(p^{r-1})} &\equiv 1 \quad (p^{r-1}), \\ g^{\varphi(p^{r-1})} &= 1 + n p^{r-1} \end{aligned}$$

mit $p \nmid n$ wegen (11). Weiter ist mit $r \geqq 2$

$$\begin{aligned} g^{\varphi(p^r)} &= (1 + n p^{r-1})^p \equiv 1 + n p^r + \frac{p(p-1)}{2} n^2 p^{2r-2} \quad (p^{r+1}) \\ &\equiv 1 + n p^r \quad (p^{r+1}) \\ &\not\equiv 1 \quad (p^{r+1}), \end{aligned}$$

und (11) ist auch richtig für $r + 1$.

Satz 2.14. *Es sei p eine ungerade Primzahl. Die prime Restklassengruppe modulo p^ν $(\nu > 1)$ ist zyklisch. Ist g eine primitive Wurzel modulo p mit $g^{p-1} \not\equiv 1$ (p^2), dann ist g auch primitive Wurzel modulo p^ν für alle $\nu \geqq 1$.*

Beweis. Nach Hilfssatz 2.4 gibt es eine primitive Wurzel g modulo p mit $g^{p-1} \not\equiv 1$ (p^2). Nehmen wir an, g gehört modulo p^ν zum Exponenten d. Aus $g^d \equiv 1$ (p^ν) folgt insbesondere $g^d \equiv 1$ (p). Da g primitive Wurzel modulo p ist, muß $(p-1) \mid d$ sein. Da andererseits $d \mid \varphi(p^\nu)$ ist und $\varphi(p^\nu) = p^{\nu-1}(p-1)$ gilt, ergibt sich $d = \varphi(p^r)$ mit $1 \leqq r \leqq \nu$. Wäre $r < \nu$, so hätten wir $d \mid \varphi(p^{r-1})$ und $g^{\varphi(p^{r-1})} \equiv 1$ (p^r) im Widerspruch zu Hilfssatz 2.5. Also ist $d = \varphi(p^\nu)$, und g ist primitive Wurzel modulo p^ν.

Wir wenden uns nun den primen Restklassengruppen modulo 2^ν $(\nu \geqq 1)$ zu. Für $\nu = 1, 2$ sind sie trivialerweise zyklisch. Aber für $\nu = 3$ ist die Gruppe $G_8 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ nicht zyklisch, da die Elemente $\bar{3}$, $\bar{5}$, $\bar{7}$ von der Ordnung 2 sind. Dieses gilt auch für die Gruppen mit $\nu \geqq 3$. Denn ist a eine beliebige ungerade Zahl, so ist für $\nu \geqq 3$ stets

$$a^{2^{\nu-2}} \equiv 1 \quad (2^\nu), \tag{12}$$

während $\varphi(2^\nu) = 2^{\nu-1}$ ist. Für $\nu = 3$ haben wir (12) schon bestätigt. Durch Induktion schließen wir aus der Richtigkeit von (12) für ν auf die Richtigkeit für $\nu + 1$:

$$a^{2^{\nu-1}} = (a^{2^{\nu-2}})^2 = (1 + k2^\nu)^2$$
$$= 1 + k2^{\nu+1} + k^2 2^{2\nu} \equiv 1 \quad (2^{\nu+1}).$$

Satz 2.15. *Die prime Restklassengruppe modulo 2^ν ist für $\nu \geqq 3$ direktes Produkt einer zyklischen Gruppe der Ordnung 2 und einer zyklischen Gruppe der Ordnung $2^{\nu-2}$. Jedes Element $\bar{a}$ der Gruppe läßt sich in der Form $\bar{a} = \overline{(-1)^r}\,\bar{5}^s$ ($r = 0, 1$; $s = 0, 1, \ldots, 2^{\nu-2} - 1$) darstellen.*

Beweis. Die Zahl -1 gehört modulo 2^ν zum Exponenten 2 und 5 wegen (12) und

$$5^{2^{\nu-3}} = (1 + 2^2)^{2^{\nu-3}} \not\equiv 1 \quad (2^\nu)$$

zum Exponenten $2^{\nu-2}$. Die Zahlen 5^s sind nach Hilfssatz 2.2 inkongruent, und aus $5^{s_1} \equiv 1 \quad (4)$, $-5^{s_2} \equiv -1 \quad (4)$ folgt auch stets $5^{s_1} \not\equiv -5^{s_2} \quad (2^\nu)$. Demzufolge bilden die $2^{\nu-1} = \varphi(2^\nu)$ Zahlen $(-1)^r 5^s$ ein primes Restsystem modulo 2^ν.

Satz 2.16. *Es sei p eine ungerade Primzahl. Ist g primitive Wurzel modulo p^ν, dann ist die ungerade der Zahlen g, $g + p^\nu$ primitive Wurzel modulo 2^ν ($\nu \geqq 1$).*

Beweis. Es bezeichne g_1 die ungerade der beiden Zahlen g, $g + p^\nu$. g_1 gehöre modulo $2p^\nu$ zum Exponenten d. Dann ist $d \mid \varphi(2p^\nu)$, und mit $\varphi(p^\nu) = \varphi(2p^\nu)$ folgt $d \leqq \varphi(p^\nu)$. Modulo p^ν ist g_1 primitive Wurzel und daher $d \geqq \varphi(p^\nu)$. Folglich ist $d = \varphi(2p^\nu)$.

Insgesamt wurde für die Moduln $m = 2, 4, p^\nu, 2p^\nu \,(p \equiv 1 \quad (2))$ die Existenz primitiver Wurzeln nachgewiesen. Jetzt werden wir zeigen, daß es für alle anderen Moduln $m > 1$ keine primitiven Wurzeln gibt. Das folgt aus nachstehendem Satz.

Satz 2.17. *Es seien m eine natürliche Zahl mit $m > 1$; $m \neq 2, 4, p^\nu, 2p^\nu \,(p \equiv 1 \quad (2), \nu \geqq 1)$ und a eine ganze Zahl mit $(a, m) = 1$.*
Dann gilt

$$a^{\frac{\varphi(m)}{2}} \equiv 1 \quad (m).$$

Beweis. Wir haben drei Fälle zu unterscheiden.

1. $m = 2^\nu$; $\nu \geqq 3$: Dieser Fall ist durch (12) bereits erledigt.
2. $m = 2^\nu p^\alpha$; $\nu \geqq 2$; $\alpha \geqq 1$: Es ist

$$\varphi(m) = 2^{\nu-1} p^{\alpha-1}(p - 1),$$

und unter den genannten Voraussetzungen ist $\frac{\varphi(m)}{2}$ durch $\varphi(2^\nu)$ und $\varphi(p^\alpha)$ teilbar. Daher ist

$$a^{\frac{\varphi(m)}{2}} \equiv 1 \quad (2^\nu),$$
$$\equiv 1 \quad (p^\alpha),$$

was der Behauptung äquivalent ist.

3. $m = 2^\nu \prod_{i=1}^{r} p_i^{\alpha_i}$; $\nu \geqq 0$; $r \geqq 2$: Analog zu 2. stellen wir aus

$$\varphi(m) = \varphi(2^\nu) \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1)$$

die Teilbarkeit von $\frac{\varphi(m)}{2}$ durch $\varphi(2^\nu)$ und $\varphi(p_i^{\alpha_i})$ $(i = 1, 2, \ldots, r)$ fest. Also entsprechend der Behauptung ist

$$\begin{aligned} a^{\frac{\varphi(m)}{2}} &\equiv 1 \quad (2^\nu), \\ &\equiv 1 \quad (p_i^{\alpha_i}) \qquad (i = 1, 2, \ldots, r). \end{aligned}$$

2.6. Die Indexrechnung

In diesem Abschnitt bezeichne $m > 1$ stets einen solchen Modul, der primitive Wurzeln besitzt, das heißt $m = 2, 4, p^\nu, 2p^\nu$ $(p \equiv 1 \quad (2), \nu \geqq 1)$. Ist g eine primitive Wurzel modulo m, so wissen wir nach dem vorangegangenen Abschnitt, daß die Zahlen $1, g, g^2, \ldots, g^{\varphi(m)-1}$ ein primes Restsystem modulo m bilden. Damit kann man jeder zu m primen Zahl a eine Zahl μ $(\mu \in \{0, 1, \ldots, \varphi(m) - 1\})$ zuordnen, so daß $a \equiv g^\mu(m)$ gilt. Das führt zu folgender Definition:

Definition 2.8. Es sei g primitive Wurzel modulo m, $(a, m) = 1$ und μ die aus der Kongruenz $a \equiv g^\mu \quad (m)$ eindeutig bestimmte Zahl der Menge $\{0, 1, \ldots, \varphi(m) - 1\}$. Dann heißt μ der *Index* der Zahl a bezüglich der Basis g modulo m, und es wird $\mu = \mathrm{ind}_g a$ geschrieben.

Sind keine Verwechslungen zu befürchten, so schreiben wir auch kürzer $\mu = \mathrm{ind}\, a$.

Die auf der Grundlage dieser Definition entwickelte *Indexrechnung* entspricht weitgehend dem bekannten Rechnen mit Logarithmen wie der folgende Satz zeigt.

Satz 2.18. *Für die Indexrechnung gelten folgende Gesetze:*

1. $\mathrm{ind}\,(ab) \equiv \mathrm{ind}\, a + \mathrm{ind}\, b \quad \big(\varphi(m)\big)$,
2. $\mathrm{ind}\, a^n \equiv n \,\mathrm{ind}\, a \quad \big(\varphi(m)\big), \qquad n \geqq 1$,
3. $\mathrm{ind}\, 1 = 0$,
4. $\mathrm{ind}_g g = 1$,
5. $\mathrm{ind}\,(-1) = \frac{1}{2}\varphi(m), \qquad m > 2$.

Beweis. Aus

$$a \equiv g^{\mathrm{ind}\, a} \quad (m), \qquad b \equiv g^{\mathrm{ind}\, b} \quad (m)$$

folgt

$$a \cdot b \equiv g^{\mathrm{ind}\, a + \mathrm{ind}\, b} \quad (m).$$

Der Vergleich mit

$$a \cdot b \equiv g^{\mathrm{ind}\,(ab)} \quad (m)$$

gibt die erste Eigenschaft. Die Eigenschaften 2 und 3 sind sofort aus 1. ablesbar. Aus $g = g^{\text{ind}_g(m)}$ ergibt sich 4. Die Aussage 5 folgt aus dem Satz von FERMAT-EULER:

$$g^{\varphi(m)} - 1 = \left(g^{\frac{\varphi(m)}{2}} - 1\right)\left(g^{\frac{\varphi(m)}{2}} + 1\right) \equiv 0 \quad (m).$$

Für $m > 2$ ist stets $2 \mid \varphi(m)$. Ist $m = 4$, so ist $g = 3$ und

$$3^{\frac{\varphi(4)}{2}} + 1 = 4 \equiv 0 \quad (4).$$

Ist $m = p^k$, so können nicht beide Faktoren durch p teilbar sein, da sie die Differenz 2 haben. Da g primitive Wurzel ist, muß also

$$g^{\frac{\varphi(m)}{2}} \equiv -1 \quad (m)$$

sein. Für $m = 2p^k$ folgt die Behauptung genauso, wenn man noch beachtet, daß g ungerade sein muß.

Für das Rechnen mit Indizes ist wie bei den Logarithmen ein Tafelwerk nötig. Wir werden eine *Indextafel* für den Modul $m = 17$ aufstellen. Weitere Tafeln findet man etwa in [13] und [19]. Es ist $\varphi(17) = 16$ und 3 eine primitive Wurzel modulo 17, da $3^2 \equiv 9$, $3^4 \equiv -4$, $3^8 \equiv -1$ modulo 17 sind. Nacheinander bestimmen wir $3^0 \equiv 1$, $3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 10$, $3^4 \equiv 13$, $3^5 \equiv 5$, $3^6 \equiv 15$, $3^7 \equiv 11$, $3^8 \equiv 16$, $3^9 \equiv 14$, $3^{10} \equiv 8$, $3^{11} \equiv 7$, $3^{12} \equiv 4$, $3^{13} \equiv 12$, $3^{14} \equiv 2$, $3^{15} \equiv 6$, $3^{16} \equiv 1$ modulo 17. Je nach Anordnung können wir uns zwei Tafeln notieren:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{ind}_3 a$	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

$\text{ind}_3 a$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

Wir wollen die Anwendung der Indexrechnung an zwei Beispielen verdeutlichen.

1. Lineare Kongruenzen:

$$ax \equiv b \quad (m), \qquad (a, m) = (b, m) = 1$$
$$\Rightarrow \text{ind}\, a + \text{ind}\, x \equiv \text{ind}\, b \quad \big(\varphi(m)\big)$$
$$\Rightarrow \text{ind}\, x \equiv \text{ind}\, b - \text{ind}\, a \quad \big(\varphi(m)\big).$$

Beispiel: $9x \equiv 7 \quad (17) \Rightarrow \text{ind}\, x \equiv \text{ind}\, 7 - \text{ind}\, 9 \equiv 11 - 2 \equiv 9 \quad (16)$

$$\Rightarrow \quad x \equiv 14 \quad (17).$$

2. Exponentialkongruenzen: Die Kongruenz

$$a^x \equiv b \quad (m), \qquad (a, m) = (b, m) = 1$$

wird auf die lineare Kongruenz

$$x \operatorname{ind} a \equiv \operatorname{ind} b \quad (\varphi(m))$$

zurückgeführt, woraus sich die Lösbarkeit für $(\varphi(m), \operatorname{ind} a) \mid \operatorname{ind} b$ ergibt.

Beispiel: $7^x \equiv 5 \quad (17) \Rightarrow x \operatorname{ind} 7 \equiv \operatorname{ind} 5 \quad (16) \Rightarrow 11x \equiv 5 \quad (16)$

$$\Rightarrow x \equiv 15 \quad (16).$$

2.7. Potenzreste

Wir wollen Aussagen über die Lösbarkeit von Kongruenzen

$$ax^n \equiv b \quad (m)$$

mit $n \geqq 2$ erzielen. Wie bei den linearen Kongruenzen können wir uns auf den Fall $(a, m) = 1$ beschränken. Da nach dem Satz von FERMAT-EULER $x^n \equiv ba^{\varphi(m)-1} \, (m)$ gilt, genügt es, den Fall der Potenzreste zu betrachten.

Definition 2.9. Es seien m, n natürliche Zahlen mit $m \geqq 2$, $n \geqq 2$, a ganze Zahl mit $(a, m) = 1$. Die Zahl a heißt n-ter *Potenzrest* modulo m, sofern die Kongruenz $x^n \equiv a \quad (m)$ lösbar ist.

Die Untersuchung derartiger Kongruenzen kann immer auf den Fall von Primzahlpotenzmoduln zurückgeführt werden. Dies geht aus dem nachfolgenden Satz hervor, der für beliebige Polynomkongruenzen formuliert wird, was den Beweis nicht komplizieren wird.

Satz 2.19. *Es sei $f(x)$ ein Polynom in x mit ganzzahligen Koeffizienten. Die Anzahl der Lösungen von*

$$f(x) \equiv 0 \quad (m), \qquad m = \prod_{i=1}^{r} p_i^{\nu_i}$$

ist $N = n_1 n_2 \cdot \cdots \cdot n_r$, wobei die n_i die Anzahl der Lösungen von $f(x) \equiv 0 \quad (p_i^{\nu_i})$ bezeichnen.

Beweis. Die Lösbarkeit der Kongruenz $f(x) \equiv 0 \quad (m)$ ist gleichbedeutend mit der Lösbarkeit des Systems

$$f(x) \equiv 0 \quad (p_i^{\nu_i}) \qquad (i = 1, 2, \ldots, r).$$

Im Falle der Lösbarkeit jeder einzelnen Kongruenz bezeichne $x \equiv c_i \quad (p_i^{\nu_i})$ eine Lösung der i-ten Kongruenz. Mit $i = 1, 2, \ldots, r$ erhält man ein lineares System von Kongruenzen, das nach Satz 2.10 eine eindeutig bestimmte Lösung modulo m besitzt. Durchlaufen die c_i alle n_i inkongruenten Lösungen, so erhält man insgesamt N Lösungen modulo m.

Zunächst wollen wir Kongruenzen betrachten, deren Moduln aus der Potenz einer ungeraden Primzahl bestehen.

Satz 2.20. *Es sei p eine ungerade Primzahl und a nicht durch p teilbar. Die Kongruenz*

$$x^n \equiv a \quad (p^r)$$

hat genau $d = \left(n, p^{r-1}(p-1)\right)$ inkongruente Lösungen, wenn $d \mid \operatorname{ind} a$. Andernfalls ist die Kongruenz unlösbar.

Beweis. Die Aussage des Satzes ist durch Anwendung von Satz 2.3 auf die sich ergebende lineare Kongruenz

$$n \operatorname{ind} x \equiv \operatorname{ind} a \quad \left(p^{r-1}(p-1)\right)$$

klar.

Beispiel: $x^3 \equiv a \quad (p), \qquad p \geqq 5, (a, p) = 1.$
Es ist $d = (3, p-1)$. Ist also $p \equiv -1 \quad (6)$, so besitzt die Kongruenz genau eine Lösung. Ist dagegen $p \equiv 1 \quad (6)$, so hat die Kongruenz entweder genau drei Lösungen oder gar keine Lösung.

Satz 2.21. *Es sei p eine ungerade Primzahl, $p \nmid a$ und $d = \left(n, p^{r-1}(p-1)\right)$. Notwendig und hinreichend für die Lösbarkeit der Kongruenz*

$$x^n \equiv a \quad (p^r)$$

ist das Bestehen der Kongruenz

$$a^{\frac{1}{d}p^{r-1}(p-1)} \equiv 1 \quad (p^r). \tag{13}$$

Beweis. Es sei g eine primitive Wurzel modulo p^r. Nach Satz 2.20 ist die Kongruenz genau dann lösbar, wenn es eine ganze Zahl h gibt mit $\operatorname{ind} a = h \cdot d$. Dann ist

$$a \equiv g^{\operatorname{ind} a} \equiv g^{h \cdot d} \quad (p^r),$$

$$a^{\frac{1}{d}p^{r-1}(p-1)} \equiv g^{hp^{r-1}(p-1)} \equiv 1 \quad (p^r).$$

Es sei umgekehrt (13) erfüllt. Mit $\mu = \operatorname{ind} a$ und $a \equiv g^{\mu} \quad (p^r)$ folgt aus (13)

$$g^{\frac{\mu}{d}p^{r-1}(p-1)} \equiv 1 \quad (p^r).$$

Hierin muß der Exponent ein Vielfaches von $p^{r-1}(p-1)$ sein, da g primitive Wurzel ist. Also ist $d \mid \mu$. Das bedeutet aber nach Satz 2.20 die Lösbarkeit der Kongruenz.

Hilfssatz 2.6. *Besitzt die natürliche Zahl $m > 1$ primitive Wurzeln und ist $t \mid \varphi(m)$, so hat die Kongruenz $x^t \equiv 1 \quad (m)$ genau t inkongruente Lösungen modulo m.*

Beweis. Für die Kongruenz $t \operatorname{ind} x \equiv 0 \quad \left(\varphi(m)\right)$ gilt $\left(t, \varphi(m)\right) = t$. Aus Satz 2.3 folgt die Behauptung.

Satz 2.22. *Ist p eine ungerade Primzahl und ist $d = \left(n, p^{r-1}(p-1)\right)$, so gibt es genau $\dfrac{1}{d}\, p^{r-1}(p-1)$ n-te Potenzreste modulo p^r.*

Beweis. Nach Satz 2.21 ist die Anzahl der Potenzreste gleich der Anzahl der Lösungen der Kongruenz (13). Nach Hilfssatz 2.6 folgt die Behauptung.

Beispiel: $x^4 \equiv a \pmod{17}$.

Es ist $d = (4,16) = 4$ und $\frac{1}{d}\, p^{r-1}(p-1) = 4$. Also gibt es vier biquadratische Reste. Es sind dies 1, 4, 13, 16.

Bei der Betrachtung des Moduls 2^ν unterscheiden wir zwischen $n \equiv 1 \pmod 2$ und $n \equiv 0 \pmod 2$.

Satz 2.23. *Es sei* $a \equiv n \equiv 1 \pmod 2$. *Dann hat die Kongruenz*

$$x^n \equiv a \pmod{2^\nu}$$

für $\nu \geqq 1$ *genau eine Lösung.*

Beweis. Wir unterscheiden die Fälle $\nu = 1$, $\nu = 2$, $\nu \geqq 3$. Für $\nu = 1$ handelt es sich um die Kongruenz $x^n \equiv 1 \pmod 2$ mit der einzigen Lösung $x \equiv 1 \pmod 2$. Für $\nu = 2$ ist $x \equiv 1 \pmod 4$ wegen der Ungeradheit von n die einzige Lösung im Fall $a \equiv 1 \pmod 4$ und $x \equiv -1 \pmod 4$ für $a \equiv -1 \pmod 4$.

Für $\nu \geqq 3$ verwenden wir Satz 2.15. Danach läßt sich a in der Form

$$a \equiv (-1)^r 5^s \pmod{2^\nu}$$

darstellen, und für x können wir den Ansatz

$$x \equiv (-1)^\varrho 5^y \pmod{2^\nu}$$

machen. Dann folgt aus

$$(-1)^{n\varrho} 5^{ny} \equiv (-1)^r 5^s \pmod{2^\nu}$$

$\varrho \equiv r \pmod 2$ bei Betrachtung modulo 4. Schließlich muß $ny \equiv s \pmod{2^{\nu-2}}$ sein, und diese lineare Kongruenz hat wegen $n \equiv 1 \pmod 2$ genau eine Lösung. Also gibt es auch genau eine Lösung x modulo 2^ν.

Satz 2.24. *Es sei* $a \equiv n \equiv 1 \pmod 2$, $\alpha \geqq 1$, $\nu \geqq 1$. *Dann hat die Kongruenz*

$$x^{2^\alpha n} \equiv a \pmod{2^\nu}$$

für $\nu < \alpha + 2$ *genau* 2^{r-1} *Lösungen, falls* $a \equiv 1 \pmod{2^\nu}$ *und für* $\nu \geqq \alpha + 2$ *genau* $2^{\alpha+1}$ *Lösungen, falls* $a \equiv 1 \pmod{2^{\alpha+2}}$. *In allen anderen Fällen ist die Kongruenz unlösbar.*

Beweis. Für $\nu = 1$ ist alles klar. Daher sei $\nu \geqq 2$. Entsprechend dem Beweis des Satzes 2.23 setzen wir

$$a \equiv (-1)^r 5^s \pmod{2^\nu}, \qquad x \equiv (-1)^\varrho 5^y \pmod{2^\nu},$$

$$5^{2^\alpha ny} \equiv (-1)^r 5^s \pmod{2^\nu}.$$

Die Betrachtung modulo 4 zeigt, daß nur $r \equiv 0 \pmod 2$ sein kann. Damit ist $a \equiv 1 \pmod 4$

notwendig für die Lösbarkeit. In diesem Fall ist

$$2^{\alpha}ny \equiv s \quad (2^{\nu-2}).$$

Jetzt trennen wir die Fälle $\nu < \alpha + 2$ und $\nu \geqq \alpha + 2$.

1. $\nu < \alpha + 2$: Die lineare Kongruenz ist genau dann lösbar, wenn $s = s'2^{\nu-2}$, also $a \equiv 1 \quad (2^{\nu})$ ist. Alle ganzen Zahlen y sind Lösungen, das heißt modulo $2^{\nu-2}$ gibt es $2^{\nu-2}$Lösungen y. Da ϱ gleich 0 oder 1 sein kann, gibt es $2^{\nu-1}$ Lösungen x.

2. $\nu \geqq \alpha + 2$: Die lineare Kongruenz ist genau dann lösbar, wenn $s = s'2^{\alpha}$, also $a \equiv 1 \quad (2^{\alpha+2})$ ist. Die sich ergebende Kongruenz

$$ny \equiv s' \quad (2^{\nu-\alpha-2})$$

hat genau eine Lösung y modulo $2^{\nu-\alpha-2}$, also 2^{α} Lösungen y modulo $2^{\nu-2}$. Mit $\varrho = 0,1$ ergeben sich $2^{\alpha+1}$ Lösungen x.

2.8. Quadratische Kongruenzen

Wir betrachten mit ganzen Zahlen a, b, c, m $\left(m > 1, a \not\equiv 0 \ (m)\right)$ die quadratische Kongruenz

$$ax^2 + bx + c \equiv 0 \quad (m).$$

Durch Multiplikation mit $4a$ kann diese Kongruenz auf die Gestalt

$$(2ax + b)^2 \equiv b^2 - 4ac \quad (4am)$$

gebracht werden. Das heißt, daß man die Auflösung quadratischer Kongruenzen völlig beherrscht, wenn man die speziellen Kongruenzen

$$x^2 \equiv a \quad (m)$$

beherrscht. Damit ist die Problematik auf die Frage nach den *quadratischen Resten* zurückgeführt. Gegenüber dem vorangegangenen Abschnitt können wir in diesem Spezialfall die Frage der Lösbarkeit vollständig beantworten. Genauer genommen ergeben sich zwei Fragen:

1. *Welche Zahlen a sind zu gegebenem m quadratischer Rest beziehungsweise Nicht-Rest?*

2. *Welche Zahlen m haben die Eigenschaft, daß ein gegebenes a quadratischer Rest oder Nicht-Rest ist?*

Während für die Beantwortung der ersten Frage relativ einfache Kriterien gegeben werden können, ist die Beantwortung der zweiten Frage recht schwierig. Sie gelingt mit Hilfe des sogenannten *quadratischen Reziprozitätsgesetzes*, welches für die Weiterentwicklung der Zahlentheorie von außerordentlicher Bedeutung war. Es wurde bereits von L. Euler auf Grund reichen Zahlenmaterials entdeckt und von A. M. Legendre (1752—1833) zum Teil bewiesen. Den ersten vollständigen Beweis gab C. F. Gauss im Jahre 1796. Von ihm selbst stammen insgesamt acht verschiedene Beweise.

Heutzutage existieren zahllose Beweisvarianten, die sich aber alle in ihrem Grundprinzip auf fünf schon bei GAUSS vorkommende Typen reduzieren lassen.

Zunächst soll gezeigt werden, daß die Behandlung von Kongruenzen $x^2 \equiv a \pmod{m}$ mit Primzahlmoduln ausreichend ist. Nach Satz 2.19 genügt es, Kongruenzen $x^2 \equiv a \pmod{p^\nu}$, p Primzahl, zu behandeln. Man kann ferner $(a, p) = 1$ annehmen. Denn wäre $p \mid a$, so hätte man $x \equiv 0 \pmod{p}$ im Fall $\nu = 1$. Für $\nu > 1$ müßte $x = py$, also $py^2 \equiv a' \pmod{p^{\nu-1}}$ $(a = pa')$ sein. Notwendig für die Lösbarkeit ist $a' = pa''$, so daß man mit $y^2 = a''$ $(p^{\nu-2})$ eine Kongruenz vom gleichen Typus erhält.

Wir betrachten also jetzt Kongruenzen

$$x^2 \equiv a \pmod{p^\nu}, \qquad (a, p) = 1. \tag{14}$$

Der Fall $p = 2$ ist durch Satz 2.24 bereits erledigt:

1. $\nu = 1$: Es existiert genau eine Lösung.
2. $\nu = 2$: a) $a \equiv 1 \pmod{4}$: Es existieren genau zwei Lösungen.
   b) $a \equiv -1 \pmod{4}$: Es gibt keine Lösung.
3. $\nu \geqq 3$: a) $a \equiv 1 \pmod{8}$: Es existieren genau vier Lösungen.
   b) $a \not\equiv 1 \pmod{8}$: Es gibt keine Lösung.

Wir wenden uns nun den ungeraden Primzahlen zu.

Satz 2.25. *Ist p eine ungerade Primzahl, so hat die Kongruenz (14) entweder keine oder genau zwei Lösungen. Ist a quadratischer Rest modulo p, so auch modulo p^ν und umgekehrt.*

Beweis. Es ist $\left(2, p^{\nu-1}(p-1)\right) = 2$. Nach Satz 2.20 hat die Kongruenz (14) genau zwei Lösungen, wenn $\operatorname{ind} a \equiv 0 \pmod{2}$ und keine Lösung, wenn $\operatorname{ind} a \equiv 1 \pmod{2}$. Wir haben dann noch zu zeigen, daß $\operatorname{ind} a$ unabhängig von ν durch 2 teilbar ist oder nicht. Es sei g eine primitive Wurzel modulo p^ν für beliebiges $\nu \geqq 1$ und $\mu_\nu = \operatorname{ind} a$ bezüglich des Moduls p^ν. Aus

$$a \equiv g^{\mu_\nu} \pmod{p^\nu}, \qquad a \equiv g^{\mu_\nu} \equiv g^{\mu_1} \pmod{p}$$

folgt $\mu_\nu \equiv \mu_1 \pmod{p-1}$ und daher $\mu_\nu \equiv \mu_1 \pmod{2}$.

Von nun an nehmen wir (14) mit $\nu = 1$ zum Gegenstand unserer Untersuchungen.

Satz 2.26. *Ist p eine ungerade Primzahl, so gibt es genausoviel quadratische Reste wie Nicht-Reste. Die quadratischen Reste sind durch $a \equiv 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2 \pmod{p}$ gegeben.*

Beweis. Die angegebenen Zahlen sind modulo p inkongruent. Denn ist $b^2 \equiv c^2 \pmod{p}$ mit $1 \leqq b, c \leqq \frac{p-1}{2}$, so ist $(b - c)(b + c) \equiv 0 \pmod{p}$. Wegen $1 < b + c < p$ folgt $b - c \equiv 0 \pmod{p}$, also $b = c$. Da $(p - k)^2 \equiv k^2 \pmod{p}$ ist, muß jeder quadratische Rest einer der Zahlen a kongruent sein. Damit ist der Satz bewiesen.

In Anlehnung an A. M. LEGENDRE drücken wir die Aussage „quadratischer Rest" oder „quadratischer Nicht-Rest" durch ein Symbol aus, das nur der Werte ± 1 fähig ist.

Definition 2.10. Es sei p eine ungerade Primzahl und $p \nmid a$. Das *Legendre-Symbol* $\left(\frac{a}{p}\right)$ (lies „a für p“) wird folgendermaßen festgelegt:

$$\left(\frac{a}{p}\right) = \begin{cases} +1, \text{ wenn } a \text{ quadratischer Rest modulo } p, \\ -1, \text{ wenn } a \text{ quadratischer Nicht-Rest modulo } p. \end{cases}$$

Es geht jetzt also darum, Regeln für die Berechnung des Symbols aufzustellen. Klar sind die Eigenschaften

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \quad \text{für} \quad a \equiv b \quad (p),$$

$$\left(\frac{a^2}{p}\right) = 1.$$

Nach dem Satz von FERMAT-EULER ist $a^{p-1} \equiv 1 \quad (p)$ und daher $a^{\frac{p-1}{2}} \equiv \pm 1 \ (p)$. Nach Satz 2.21 ist $a^{\frac{p-1}{2}} \equiv 1 \quad (p)$ notwendig und hinreichend für die Lösbarkeit der Kongruenz $x^2 \equiv a \quad (p)$. Damit haben wir den folgenden als *Eulersches Kriterium* bezeichneten Satz:

Satz 2.27.

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \quad (p).$$

Aus diesem Kriterium kann schon eine Reihe wichtiger Schlüsse gezogen werden.

Satz 2.28.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Beweis.

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \quad (p).$$

Satz 2.29.

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

Beweis. Die erste Formel folgt sofort, wenn man in Satz 2.27 $a = -1$ setzt. Zum Beweis der zweiten Formel betrachten wir das Produkt

$$\prod_{k=1}^{\frac{p-1}{2}} (-1)^k k = \left(\frac{p-1}{2}\right)! \ (-1)^{\frac{p^2-1}{8}}.$$

Ist in dem Produkt k ungerade, so ersetzen wir $-k$ modulo p durch $p-k$ und erhalten

$$\prod_{k=1}^{\frac{p-1}{2}} (-1)^k k \equiv 2 \cdot 4 \cdot 6 \cdot \cdots \cdot (p-1) = \left(\frac{p-1}{2}\right)! \, 2^{\frac{p-1}{2}} \quad (p).$$

Da $p \nmid \left(\frac{p-1}{2}\right)!$, folgt

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \quad (p)$$

und nach dem Eulerschen Kriterium die Behauptung.

Wir sehen uns zwei *Beispiele zur Anwendung des Eulerschen Kriteriums* an:

1. $x^2 \equiv -1 \quad (p)$:

Wegen

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{für } p \equiv 1 \quad (4), \\ -1 & \text{für } p \equiv -1 \quad (4) \end{cases}$$

ist die Kongruenz für $p \equiv 1 \quad (4)$ lösbar, für $p \equiv -1 \quad (4)$ unlösbar. Im Falle der Lösbarkeit sind die Lösungen durch

$$x \equiv \pm \left(\frac{p-1}{2}\right)! \quad (p)$$

gegeben. Denn aus

$$\left(\frac{p-1}{2}\right)! = (-1)(-2) \cdot \cdots \cdot \left(-\frac{p-1}{2}\right)(-1)^{\frac{p-1}{2}}$$

$$\equiv (p-1)(p-2) \cdot \cdots \cdot \left(p - \frac{p-1}{2}\right) \quad (p)$$

folgt

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (p-1)! \equiv -1 \quad (p)$$

nach dem Satz von Wilson.

2. $x^2 \equiv a \quad (p), \qquad p \equiv 3 \quad (4), \qquad \left(\frac{a}{p}\right) = +1$:

Die Lösungen sind

$$x \equiv \pm a^{\frac{p+1}{4}} \quad (p),$$

denn

$$\left(a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} a \equiv \left(\frac{a}{p}\right) a \equiv a \quad (p).$$

Obwohl das Eulersche Kriterium eine Methode zur Berechnung von $\left(\frac{a}{p}\right)$ gibt, bringt es doch für große a erhebliche Mühe mit sich. Eine Vereinfachung bietet der auf C. F. Gauss zurückgehende folgende Satz.

Satz 2.30 (Gaußsches Lemma). *Es sei p eine ungerade Primzahl und $p \nmid a$. Man reduziere die $\frac{p-1}{2}$ Zahlen*

$$a, 2a, \ldots, \frac{p-1}{2}\, a \tag{15}$$

modulo p so, daß ihre Reste zwischen 0 und p liegen. Es sei μ die Anzahl derjenigen Reste, die größer als $\frac{p}{2}$ sind. Dann gilt

$$\left(\frac{a}{p}\right) = (-1)^{\mu}.$$

Beweis. Die gemäß der Anweisung modulo p reduzierten Zahlen (15) verteilen wir auf zwei disjunkte Mengen. Die Menge $A = \{a_1, a_2, \ldots, a_k\}$ enthalte diejenigen Zahlen a_i mit $0 < a_i < \frac{p}{2}$ und die Menge $B = \{b_1, b_2, \ldots, b_\mu\}$ die Zahlen b_i mit $\frac{p}{2} < b_i < p$. Da die Zahlen (15) modulo p inkongruent sind, gilt $a_i \neq a_j$ und $b_i \neq b_j$ für $i \neq j$, und es ist $k + \mu = \frac{p-1}{2}$. Kann $a_i = p - b_j$ sein? Dann muß es Zahlen x, y mit $1 \leqq x, y \leqq \frac{p-1}{2}$ geben mit $xa \equiv p - ya \pmod p$ oder $(x + y)\, a \equiv 0 \pmod p$. Da $p \nmid a$, ist $x + y \equiv 0 \pmod p$. Das ist aber wegen $0 < x + y < p$ unmöglich. Daher bildet die Vereinigung der Mengen A und $\{p - b_1, p - b_2, \ldots, p - b_\mu\}$ die Menge $\left\{1, 2, \ldots, \frac{p-1}{2}\right\}$. Damit haben wir

$$\left(\frac{p-1}{2}\right)! = \prod_{n=1}^{k} a_n \prod_{m=1}^{\mu} (p - b_m) \equiv (-1)^{\mu} \prod_{n=1}^{k} a_n \prod_{m=1}^{\mu} b_m \pmod p$$

$$\equiv (-1)^{\mu} \prod_{r=1}^{\frac{p-1}{2}} (ra) = (-1)^{\mu} \left(\frac{p-1}{2}\right)!\, a^{\frac{p-1}{2}} \pmod p$$

und

$$(-1)^{\mu} \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p,$$

was der Behauptung entspricht.

Eine Vereinfachung in Anwendung des Gaußschen Lemmas können wir noch erzielen, wenn wir μ modulo 2 betrachten. Bezeichnet $[x]$ das größte Ganze von x, so ist

für $p \nmid na$

$$na = \left[\frac{na}{p}\right] p + r_n, \qquad 1 \leqq r_n \leqq p-1.$$

Durch Summation über n von 1 bis $\frac{p-1}{2}$ ergibt sich

$$\frac{p^2-1}{8}\, a = \sum_{n=1}^{\frac{p-1}{2}} \left(\left[\frac{na}{p}\right] p + r_n\right)$$

$$= p \sum_{n=1}^{\frac{p-1}{2}} \left[\frac{na}{p}\right] + \sum_{n=1}^{k} a_n + \sum_{m=1}^{\mu} b_m,$$

wobei a_n, b_m, k, μ die obige Bedeutung haben. Weiter ist

$$\frac{p^2-1}{8}\, a = p \sum_{n=1}^{\frac{p-1}{2}} \left[\frac{na}{p}\right] + \sum_{n=1}^{k} a_n + \sum_{m=1}^{\mu} (p - b_m) - p\mu + 2 \sum_{m=1}^{\mu} b_m$$

$$\equiv - \sum_{n=1}^{\frac{p-1}{2}} \left[\frac{na}{p}\right] + \frac{p^2-1}{8} + \mu \pmod 2,$$

also

$$\mu \equiv \sum_{n=1}^{\frac{p-1}{2}} \left[\frac{na}{p}\right] + \frac{p^2-1}{8}\,(a-1) \pmod 2.$$

Für $a = 2$ erhalten wir hieraus das schon bekannte Ergebnis für $\left(\frac{2}{p}\right)$ des Satzes 2.29 und für $a \equiv 1 \pmod 2$ den folgenden Satz:

Satz 2.31. *Für ungerades a ist*

$$\left(\frac{a}{p}\right) = (-1)^m, \qquad m = \sum_{n=1}^{\frac{p-1}{2}} \left[\frac{na}{p}\right].$$

Das angekündigte quadratische Reziprozitätsgesetz erreichen wir jetzt schnell über den Hilfssatz:

Hilfssatz 2.7. *Für $a \equiv b \equiv 1 \pmod 2$; $a, b \geqq 3$, $(a, b) = 1$ gilt*

$$\sum_{m=1}^{\frac{a-1}{2}} \left[\frac{bm}{a}\right] + \sum_{n=1}^{\frac{b-1}{2}} \left[\frac{an}{b}\right] = \frac{a-1}{2} \cdot \frac{b-1}{2}. \tag{16}$$

Beweis. Wir betrachten die Zahlen $bm - an$ mit $m = 1, 2, \ldots, \frac{a-1}{2}$, $n = 1, 2, \ldots, \frac{b-1}{2}$. Ihre Anzahl $\frac{a-1}{2} \cdot \frac{b-1}{2}$ ist gleich der rechten Seite von (16). Die

linke Seite von (16) erhalten wir durch eine veränderte Abzählung. Die Anzahl der Zahlen mit $bm - an = 0$ ist 0, da aus $(a, b) = 1 m = at, n = bt$ folgt, was nicht möglich sein kann. Die Anzahl der Zahlen mit $bm - an > 0$ ist bei festem m durch $\left[\frac{bm}{a}\right]$ gegeben und insgesamt

$$\sum_{m=1}^{\frac{a-1}{2}} \left[\frac{bm}{a}\right].$$

Die analoge Betrachtung der Zahlen mit $bm - an < 0$ gibt die zweite Summe auf der linken Seite von (16).

Satz 2.32 (Gauss). *Sind p, q verschiedene ungerade Primzahlen, dann besteht das quadratische Reziprozitätsgesetz*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Beweis. Nach Satz 2.31 ist

$$\left(\frac{q}{p}\right) = (-1)^{m_1}, \quad \left(\frac{p}{q}\right) = (-1)^{m_2}$$

mit

$$m_1 = \sum_{n_1=1}^{\frac{p-1}{2}} \left[\frac{qn_1}{p}\right], \qquad m_2 = \sum_{n_2=1}^{\frac{q-1}{2}} \left[\frac{pn_2}{q}\right].$$

Aus (16) folgt sofort die Behauptung.

Zusammenfassung: *Die folgenden Eigenschaften ermöglichen die Berechnung eines jeden Legendre-Symbols:*

A. $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ für $a \equiv b \pmod p$.

B. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

C. *Quadratisches Reziprozitätsgesetz:*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

D. 1. *Ergänzungssatz zum quadratischen Reziprozitätsgesetz:*

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

E. 2. *Ergänzungssatz zum quadratischen Reziprozitätsgesetz:*

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

Beispiele:

1. Ist 74 quadratischer Rest modulo 131?

$$B \Rightarrow \left(\frac{74}{131}\right) = \left(\frac{2}{131}\right)\left(\frac{37}{131}\right).$$

$$E \Rightarrow \left(\frac{2}{131}\right) = (-1)^{\frac{131^2-1}{8}} = -1.$$

$$C \Rightarrow \left(\frac{37}{131}\right) = (-1)^{\frac{131-1}{2}\cdot\frac{37-1}{2}}\left(\frac{131}{37}\right) = \left(\frac{131}{37}\right).$$

$$A \wedge B \Rightarrow \left(\frac{131}{37}\right) = \left(\frac{20}{37}\right) = \left(\frac{2^2}{37}\right)\left(\frac{5}{37}\right) = \left(\frac{5}{37}\right).$$

$$C \Rightarrow \left(\frac{5}{37}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{37-1}{2}}\left(\frac{37}{5}\right) = \left(\frac{37}{5}\right).$$

$$A \wedge E \Rightarrow \left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1.$$

Die Eintragung aller Teilergebnisse gibt $\left(\frac{74}{131}\right) = +1$, so daß 74 quadratischer Rest modulo 131 ist.

2. Für welche Primzahlen p ist 3 quadratischer Rest beziehungsweise Nicht-Rest?

$$C \Rightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}}\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right).$$

$$p = 1 + 6k \Rightarrow \left(\frac{3}{p}\right) = (-1)^k.$$

$$p = -1 + 6k \Rightarrow \left(\frac{3}{p}\right) = (-1)^{k+1}\left(\frac{-1}{3}\right) = (-1)^k.$$

Damit ist 3 für $p \equiv \pm 1 \pmod{12}$ quadratischer Rest und für $p \equiv \pm 5 \pmod{12}$ quadratischer Nicht-Rest.

2.9. Aufgaben

1. Es ist zu zeigen: Eine natürliche Zahl ist genau dann durch 13, 17, 19 teilbar, wenn die Summe aus dem 4fachen, (-5)-fachen, 2fachen der letzten Ziffer der Dezimalbruchentwicklung und der aus den restlichen Ziffern gebildeten Zahl durch 13, 17, 19 teilbar ist.
2. Man bestimme sämtliche Lösungen der folgenden diophantischen Gleichungen:

   a) $255x + 83y = 202$,
   b) $137952x + 1743x = 415612$,
   c) $10x + 18y + 15z = 404$.

3. Man bestimme die Menge der Primteiler der Zahlen 9, 99, 999, ...
4. Es werde die Folge n^n $(n = 1, 2, \ldots)$ modulo p betrachtet, wobei p eine Primzahl bedeute. Es ist die Periodizität der Restklassenfolge nachzuweisen und die Periodenlänge zu bestimmen.
5. Man bestimme alle n mit $\varphi(n) = 1, 2, 3, 4, 5, 6, 14$.
6. Es bezeichne p_n die n-te Primzahl. Man zeige:

   a) $\dfrac{\varphi(p_n!)}{p_n!} \cdot \dfrac{p_{n-1}!}{\varphi(p_{n-1}!)} = 1 - \dfrac{1}{p_n}$.

   b) Ist $k = \prod_{i=1}^{n} p_i^{\nu_i}$

   mit $\nu_i \geqq 1 \quad (i = 1, 2, \ldots, n)$, so gilt

   $$\frac{\varphi(k)}{k} = \frac{\varphi(p_n!)}{p_n!}.$$

7. Man zeige: Für alle natürlichen Zahlen n gilt $\varphi(n) \geqq \frac{1}{2}\sqrt{n}$.
8. Man zeige: Für alle natürlichen Zahlen n gilt $\varphi(n) \leqq n - \sqrt{n}$.
9. Man zeige: Es gibt unendlich viele natürliche Zahlen n mit $\varphi(n) > \varphi(n+1)$.
10. Man beweise die Identität

$$\varphi(n) = \sum_{k=1}^{n} \left[\frac{1}{(n,\ k)}\right].$$

11. Es sind alle primitiven Wurzeln modulo 17 zu bestimmen.
12. Es sind die folgenden Kongruenzen zu lösen:

    a) $45x \equiv 28 \pmod{17}$,
    b) $x^7 \equiv 10 \pmod{17}$,
    c) $13^x \equiv 16 \pmod{17}$.

13. Man berechne die Legendre-Symbole $\left(\frac{10}{13}\right)$, $\left(\frac{26}{59}\right)$, $\left(\frac{-209}{719}\right)$, $\left(\frac{3267}{5563}\right)$.
14. Man löse, soweit möglich, die folgenden Kongruenzen:

    a) $3x^2 + 5x + 1 \equiv 0 \pmod{7}$,
    b) $4x^2 + 2x + 3 \equiv 0 \pmod{15}$,
    c) $x^3 - 3x + 2 \equiv 0 \pmod{6}$,
    d) $3x^2 + 7x + 1 \equiv 0 \pmod{9}$.

15. Für welche Primzahlen p ist $x^3 \equiv 1 \pmod{p}$ nichttrivial lösbar?
16. Für welche Primzahlen ist a) 4, b) -1 biquadratischer Rest?

3. Endliche abelsche Gruppen

Die im vorangegangenen Kapitel erfolgte vollständige Beschreibung der primen Restklassengruppe modulo m als direktes Produkt zyklischer Gruppen ordnet sich einem allgemeinen Satz der Algebra über endliche abelsche Gruppen unter. Es würde hier zu weit führen, die algebraischen Grundlagen umfassend zu entwickeln. Es sei diesbezüglich auf den Band 3, Algebra, der Studienbücherei verwiesen. Dennoch verbindet sich hiermit eine der Natur nach zahlentheoretische Fragestellung nach der Anzahl der wesentlich verschiedenen abelschen Gruppen gegebener Ordnung, die nachfolgend angeschnitten werden soll.

Ferner sollen Funktionen über endliche abelsche Gruppen erklärt und untersucht werden. Durch Spezialisierung auf die prime Restklassengruppe modulo p wird sich zeigen, daß sich das Legendre-Symbol in harmonischer Weise einordnet. Durch den Einbau dieses Symbols in trigonometrische Summen wird sich ein neuer Beweis des quadratischen Reziprozitätsgesetzes ergeben, der sich nicht mehr auf das Gaußsche Lemma stützt und der somit einem tieferen Verständnis des vielleicht wichtigsten Gesetzes der Zahlentheorie dient.

3.1. Nichtisomorphe endliche abelsche Gruppen

Bekanntlich heißt eine abelsche Gruppe G *direktes Produkt* ihrer Untergruppen $A_1, A_2, \ldots, A_r$, wenn sich jedes Element $g \in G$ auf genau eine Weise in der Form $g = a_1 a_2 \cdot \cdots \cdot a_r$ $(a_i \in A_i, i = 1, 2, \ldots, r)$ darstellen läßt. Man schreibt dann auch $G = A_1 \times A_2 \times \cdots \times A_r$. Mit Hilfe des direkten Produktes kann dann nicht nur wie im vorigen Kapitel die Struktur der primen Restklassengruppen, sondern die einer jeden endlichen abelschen Gruppe beschrieben werden.

Satz 3.1 (Hauptsatz für endliche abelsche Gruppen). *Jede endliche abelsche Gruppe ist das direkte Produkt zyklischer Gruppen von Primzahlpotenzordnung.*

Darüber hinaus gilt:

Satz 3.2. *Die Darstellung einer endlichen abelschen Gruppe von Primzahlpotenzordnung als direktes Produkt zyklischer Gruppen ist, abgesehen von der Reihenfolge der Faktoren, eindeutig.*

Hinsichtlich der Beweise der beiden Sätze sei auf [5] verwiesen.

Wir wenden uns nun der zahlentheoretischen Fragestellung, der Frage nach der *Anzahl der nicht-isomorphen abelschen Gruppen einer gegebenen Ordnung*, zu. Die beiden obigen Sätze geben uns die Möglichkeit, diese Frage in Angriff zu nehmen.

Definition 3.1. Es bezeichne $a(n)$ die Anzahl der nicht-isomorphen abelschen Gruppen der Ordnung n.

Es ist also $a(n)$ eine für alle natürlichen Zahlen erklärte Funktion, und speziell ist $a(1) = 1$. Die beiden Sätze geben eine Anweisung, wie man alle wesentlich verschiedenen abelschen Gruppen einer gegebenen Ordnung n angeben kann. Man zerlege die Zahl n auf irgendeine Art in ein Produkt von Primzahlpotenzen. Zu jeder derartigen Zerlegung gibt es genau eine Gruppe. So gibt es zu jeder Primzahlordnung p genau eine abelsche Gruppe, nämlich die zyklische Gruppe der Ordnung p. Zu $n = p^2$ gibt es genau zwei abelsche Gruppen, und zwar die zyklische Gruppe der Ordnung p^2 und das direkte Produkt zweier zyklischer Gruppen der Ordnung p. Allgemein erhält man zu $n = p^m$ so viele abelsche Gruppen wie sich m als Summe von natürlichen Zahlen darstellen läßt, wobei die Reihenfolge der Summanden keine Rolle spielt. Daraus ergibt sich noch insbesondere die Eigenschaft

$$a(mn) = a(m)\, a(n) \quad \text{für} \quad (m, n) = 1.$$

Zieht man die kanonische Zerlegung von n in Primzahlpotenzen

$$n = \prod_{i=1}^{r} p_i^{\nu_i} \tag{1}$$

heran, so ist also

$$a(n) = \prod_{i=1}^{r} a(p_i^{\nu_i}). \tag{2}$$

Es genügt daher, $a(n)$ für eine Primzahlpotenz $n = p^\nu$ zu untersuchen. Das gibt Veranlassung zu der folgenden Definition.

Definition 3.2. Jede Darstellung einer natürlichen Zahl n als Summe von natürlichen Zahlen, wobei die Reihenfolge der Summanden keine Rolle spielt, heißt eine *Partition* von n. Mit $P(n)$ werde die *Anzahl der Partitionen* von n bezeichnet.

Wir geben ein paar Beispiele an. Die Zahl 1 besitzt die einzige Partition 1. Für die Zahl 2 finden wir die Möglichkeiten $2,\ 1 + 1$; für die Zahl 3 haben wir $3,\ 2 + 1,\ 1 + 1 + 1$; für die Zahl 4 geben wir $4,\ 3 + 1,\ 2 + 2,\ 2 + 1 + 1,\ 1 + 1 + 1 + 1$ an. Wir notieren die folgende Tabelle:

n	1	2	3	4	5	6	7	8	9	10	11
$P(n)$	1	2	3	5	7	11	15	22	30	42	56

Daraus gewinnen wir für $a(n)$, worin p eine beliebige Primzahl bedeutet:

n	1	2	3	4	5	6	7	8	9	10	p	p^2	p^3	p^4	p^5
$a(n)$	1	1	1	2	1	1	1	3	2	1	1	2	3	5	7

Die kurze Tabelle für $P(n)$ zeigt schon, daß diese Funktion mit n enorm wächst. Wir überlegen uns eine grobe, aber einfache Abschätzung von $P(n)$. Schreiben wir die Partitionen von n auf, so können wir dies allgemein wie in den Beispielen tun. Zunächst ist n eine Partition. Dann gibt es $P(1)$ Partitionen, die mit $n-1$ beginnen; $P(2)$ Partitionen, die mit $n-2$ beginnen. Allgemein gibt es $P(k)$ Partitionen, die mit $n-k$ beginnen, sofern $k \leqq n-k$ ist. Wird $k > n-k$, so schätzen wir die Anzahl der bestehenden Möglichkeiten nach oben ebenfalls mit $P(k)$ ab. Insgesamt ist

$$P(n) \leqq 1 + \sum_{k=1}^{n-1} P(k).$$

Aus $P(1) = 1$ folgt hieraus durch Induktion $P(n) \leqq 2^{n-1}$. Wir übertragen diese Abschätzung auf $a(n)$. Nach (1), (2) und der Definition von $P(n)$ ist

$$a(n) = \prod_{i=1}^{r} P(\nu_i) \tag{3}$$

und daher

$$a(n) \leqq 2^{\nu_1+\nu_2+\cdots+\nu_r-r}. \tag{4}$$

Zur Formulierung des Ergebnisses führen wir noch die folgenden Funktionen ein.

Definition 3.3. Es bezeichne $\Omega(n)$ die *Anzahl der Primfaktoren* von n und $\omega(n)$ die *Anzahl der verschiedenen Primfaktoren* von n.

Mit diesen Funktionen ergibt sich aus (4):

Satz 3.3.

$$a(n) \leqq 2^{\Omega(n)-\omega(n)}.$$

Für quadratfreies n ist wegen $\Omega(n) = \omega(n)$ stets $a(n) = 1$. Beachtet man die Abschätzung

$$n = \prod_{i=1}^{r} p_i^{\nu_i} \geqq 2^{\Omega(n)},$$

so sieht man für $n > 1$

$$a(n) \leqq n \cdot 2^{-\omega(n)} \leqq \frac{n}{2}.$$

In Kapitel 7 werden wir wesentlich genauere Abschätzungen für $a(n)$ vornehmen können. Die dazu benötigten Hilfsmittel stehen uns an dieser Stelle noch nicht zur Verfügung.

3.2. Charaktere endlicher abelscher Gruppen

Definition 3.4. Ein *Charakter* χ einer endlichen abelschen Gruppe G ist eine auf G erklärte, komplexwertige nicht identisch verschwindende Funktion mit der Eigenschaft

$$\chi(ab) = \chi(a)\,\chi(b)$$

für alle $a, b \in G$.

Einfache Eigenschaften der Charaktere:

1. Für alle $a \in G$ ist $\chi(a) \neq 0$.

Es bezeichne e das Einselement von G und a^{-1} das zu a inverse Element. Nehmen wir an, es existiert ein Element $c \in G$ mit $\chi(c) = 0$. Dann ist $\chi(e) = \chi(cc^{-1}) = \chi(c)\,\chi(c^{-1}) = 0$ und für beliebiges $a \in G$ $\chi(a) = \chi(e)\,\chi(a) = 0$ entgegen der Voraussetzung, daß χ nicht die identisch verschwindende Funktion sein soll.

2. $\chi(e) = \chi(e^2) = \chi(e)\,\chi(e) \Rightarrow \chi(e) = 1$.

3. Die sämtlichen Lösungen z_ν der Gleichung $z^n - 1 = 0$, $n \in \mathbf{N}$, bilden die n-ten Einheitswurzeln

$$z_\nu = e^{2\pi i \frac{\nu}{n}}; \qquad \nu = 1, 2, \ldots, n.$$

Hat die Gruppe G die Ordnung n, so ist $a^n = e$ für jedes $a \in G$. Daher ist $\chi(a)^n = \chi(a^n) = \chi(e) = 1$, und *jeder Charakter ist eine n-te Einheitswurzel*. Der Charakter χ_1 mit der Eigenschaft $\chi_1(a) = 1$ für alle $a \in G$ heißt der *Hauptcharakter* von G.

Satz 3.4. *Eine abelsche Gruppe der Ordnung n besitzt genau n verschiedene Charaktere.*

Beweis. Wir führen den Beweis zunächst für eine zyklische Gruppe G. Die Gruppe wird dann durch die Potenzen $a, a^2, \ldots, a^n = e$ eines Elementes gebildet. Ein Charakter χ von G ist wegen $\chi(a^r) = \chi(a)^r$ durch die Angabe des Wertes $\chi(a)$ vollständig bestimmt. Wegen $a^n = e$ ist $\chi(a)^n = 1$, also $\chi(a)$ eine n-te Einheitswurzel. Da es nur n verschiedene n-te Einheitswurzeln gibt, kann es also höchstens n verschiedene Charaktere geben. Umgekehrt definiert aber jede n-te Einheitswurzel ϱ durch die Festlegung $\chi(a) = \varrho$ einen Charakter. Denn aus $a^{n_1}a^{n_2} = a^{n_3}$ folgt $n_1 + n_2 \equiv n_3 \quad (n)$ und $\varrho^{n_1}\varrho^{n_2} = \varrho^{n_3}$. Somit gibt es genau n verschiedene Charaktere.

Zum Beweis für beliebige endliche abelsche Gruppen ziehen wir den Satz 3.1 heran. Danach läßt sich G als direktes Produkt $G = G_1 \times G_2 \times \cdots \times G_k$ von zyklischen Gruppen $G_1, G_2, \ldots, G_k$ darstellen. Haben die Gruppen G_j die Ordnungen n_j ($j = 1, 2, \ldots, k$), so hat die Gruppe G die Ordnung $n = n_1 n_2 \cdot \cdots \cdot n_k$. Bilden a_j die erzeugenden Elemente von G_j, so läßt sich jedes Element $a \in G$ eindeutig in der Form $a = a_1^{r_1} \times a_2^{r_2} \cdot \cdots \cdot a_k^{r_k}$ ($0 \leqq r_j \leqq n_j - 1$; $j = 1, 2, \ldots, k$) darstellen. Für jeden Charakter χ von G ist $\chi(a) = \chi(a_1)^{r_1}\,\chi(a_2)^{r_2} \cdot \cdots \cdot \chi(a_k)^{r_k}$. Bezeichnet ϱ_j eine n_j-te Einheitswurzel, so ist demzufolge durch die Vorgaben $\chi(a_j) = \varrho_j$ der Charakter χ von G eindeutig bestimmt. Da ϱ_j genau n_j verschiedene Werte annehmen kann, gibt es genau $n = n_1 n_2 \cdot \cdots \cdot n_k$ verschiedene Charaktere von G.

Die n verschiedenen Charaktere einer abelschen Gruppe der Ordnung n werden wir mit $\chi_1, \chi_2, \ldots, \chi_n$ bezeichnen. Dabei sei χ_1 der Hauptcharakter.

Wir definieren das „Produkt" zweier Charaktere χ_s, χ_t von G durch die Festsetzung $(\chi_s\chi_t)(a) := \chi_s(a)\,\chi_t(a)$, $a \in G$. Dann ist auch $\chi_s\chi_t$ ein Charakter von G, was aus

$$\begin{aligned}(\chi_s\chi_t)(ab) &= \chi_s(ab)\,\chi_t(ab) = \chi_s(a)\,\chi_t(a)\,\chi_s(b)\,\chi_t(b)\\ &= (\chi_s\chi_t)(a)\,(\chi_s\chi_t)(b)\end{aligned}$$

unmittelbar folgt. Daraus erkennt man sofort, daß die Charaktere von G selbst eine abelsche Gruppe G^*, die Charaktergruppe von G, bilden. Das Einselement bildet der Hauptcharakter χ_1. Der zu χ inverse Charakter χ^{-1} ist durch $\chi^{-1}(a) = \dfrac{1}{\chi(a)}$ gegeben. Wegen $|\chi(a)| = 1$ ist $\chi^{-1}(a) = \overline{\chi(a)}$, wobei der Strich den zu $\chi(a)$ konjugiert komplexen Wert andeuten soll.

Satz 3.5. *Die Charaktergruppe G^* einer endlichen abelschen Gruppe G ist zu G isomorph.*

Beweis. Ist G von der Ordnung n, so nach Satz 3.4 auch G^*. Es sei entsprechend einer direkten Produktzerlegung von G

$$a = a_1^{r_1}a_2^{r_2}\cdot\ldots\cdot a_k^{r_k} \qquad (0 \leqq r_j \leqq n_j - 1,\ j = 1, 2, \ldots, k)$$

mit $n = n_1n_2\cdot\ldots\cdot n_k$ eine Basisdarstellung der Elemente von G. Ist ϱ_j eine primitive n_j-te Einheitswurzel, das heißt $\varrho_j^{r_j} \neq 1$ für $0 < r_j < n_j$ und $\varrho_j^{n_j} = 1$, so läßt sich jede n_j-te Einheitswurzel in der Gestalt $\varrho_j^{s_j}$ darstellen, wobei s_j modulo n_j festgelegt ist. Demnach gilt

$$\chi(a) = \varrho_1^{r_1s_1}\varrho_2^{r_2s_2}\cdot\ldots\cdot\varrho_k^{r_ks_k}.$$

Damit ist jedem Charakter $\chi \in G^*$ eindeutig ein Exponentensystem $(s_1, s_2, \ldots, s_k)$ zugeordnet. Die Abbildung dieses Charakters auf das Element $b = a_1^{s_1}a_2^{s_2}\cdot\ldots\cdot a_k^{s_k}$ liefert offensichtlich einen Isomorphismus zwischen G^* und G.

Satz 3.6. *Es seien G eine endliche abelsche Gruppe der Ordnung n mit den Elementen $a_1, a_2, \ldots, a_n$ und G^* die zugehörige Charaktergruppe mit den Elementen χ_1 (Hauptcharakter), $\chi_2, \ldots, \chi_n$. Dann ist*

$$\sum_{\nu=1}^{n}\chi_r(a_\nu) = \begin{cases} n & \text{für } r = 1,\\ 0 & \text{für } r > 1,\end{cases} \tag{5}$$

$$\sum_{\nu=1}^{n}\chi_\nu(a_r) = \begin{cases} n & \text{für } a_r = e,\\ 0 & \text{für } a_r \neq e.\end{cases} \tag{6}$$

Bemerkung. Ersetzt man in (5) χ_r durch $\chi_r\overline{\chi}_s$ und in (6) a_r durch $a_ra_s^{-1}$, so erhält man die *Orthogonalitätsrelationen*

$$\sum_{\nu=1}^{n}\chi_r(a_\nu)\,\overline{\chi_s(a_\nu)} = \begin{cases} n & \text{für } r = s,\\ 0 & \text{für } r \neq s,\end{cases} \tag{7}$$

$$\sum_{\nu=1}^{n}\chi_\nu(a_r)\,\overline{\chi_\nu(a_s)} = \begin{cases} n & \text{für } r = s,\\ 0 & \text{für } r \neq s.\end{cases} \tag{8}$$

Beweis. Die Behauptung (5) ist für $r = 1$ sicher richtig. Sei jetzt $r > 1$. Es gibt ein Element $b \in G$ mit $\chi_r(b) \neq 1$. Mit a_ν durchläuft ba_ν die volle Gruppe G. Daher ist

$$S_1 = \sum_{\nu=1}^{n} \chi_r(ba_\nu) = \sum_{\nu=1}^{n} \chi_r(b)\,\chi_r(a_\nu) = \chi_r(b)\,S_1$$

und folglich $S_1 = 0$.

Die Behauptung (6) ist für $a_r = e$ wieder klar. Also sei $a_r \neq e$ angenommen. Wir möchten entsprechend dem ersten Teil des Beweises zu a_r einen Charakter $\chi' \in G^*$ mit $\chi'(a_r) \neq 1$ angeben. Die Existenz eines solchen Charakters geht aus folgendem hervor: Es bezeichne D die Determinante

$$D = \|\chi_i(a_j)\| \qquad (i, j = 1, 2, \ldots, n),$$

worin i den Zeilenindex und j den Spaltenindex darstellen. Wegen (7) ist $D\overline{D} = n^n$, also D von 0 verschieden. Demnach können in D auch keine zwei Spalten übereinstimmen. Weil $\chi(e) = 1$ für alle Charaktere gilt, muß in der r-ten Spalte wenigstens einmal $\chi(a_r) \neq 1$ sein. Also gibt es ein $\chi' \in G^*$ mit $\chi'(a_r) \neq 1$. Dann durchläuft aber mit χ_ν auch $\chi'\chi_\nu$ die volle Gruppe G^*, und es ist

$$S_2 = \sum_{\nu=1}^{n} (\chi'\chi_\nu)\,(a_r) = \sum_{\nu=1}^{n} \chi'(a_r)\,\chi_\nu(a_r) = \chi'(a_r)\,S_2,$$

also $S_2 = 0$.

3.3. Restklassencharaktere

Wir wenden nun die Ergebnisse des vorangegangenen Abschnitts auf die prime Restklassengruppe modulo m an: Diese mit G_m bezeichnete Gruppe ist eine endliche abelsche Gruppe der Ordnung $\varphi(m)$. Ihre Charaktere sind also über die primen Restklassen $\bar{a} = \{x : x \in \mathbf{Z},\ x \equiv a \pmod m\}$ mit $(a, m) = 1$ erklärt. Sie können durch die folgenden Festlegungen als Funktionen über alle ganzen Zahlen aufgefaßt werden. Es sei $x \in \mathbf{Z}$ und $(x, m) = 1$. Wir setzen $\chi(x) := \chi(\bar{a})$, wenn $x \in \bar{a}$. Dann ist natürlich $\chi(x) = \chi(y)$ für $x \equiv y \pmod m$. Für $(x, m) = (y, m) = 1$ ist ebenfalls $\chi(xy) = \chi(x)\,\chi(y)$. Da $\chi(\bar{a}) \neq 0$ für jede prime Restklasse $\bar{a}$ ist, haben wir bei der neuen Vereinbarung $\chi(x) \neq 0$ für alle Zahlen x mit $(x, m) = 1$. Also liegt es noch nahe, $\chi(x) = 0$ für $(x, m) > 1$ zu setzen. Zusammenfassend definieren wir:

Definition 3.5. Ein *Restklassencharakter* modulo m ist eine über $\mathbf{Z}$ erklärte Funktion mit den Eigenschaften

$$\begin{aligned}
&\chi(a) = \chi(b) && \text{für} \quad a \equiv b \pmod m,\\
&\chi(ab) = \chi(a)\,\chi(b) && \text{für alle} \quad a, b \in \mathbf{Z},\\
&\chi(a) = 0 && \text{für} \quad (a, m) > 1,\\
&\chi(a) \neq 0 && \text{für} \quad (a, m) = 1.
\end{aligned}$$

Aus dem Abschnitt 3.2. entnehmen wir: Es gibt $\varphi(m)$ Restklassencharaktere modulo m. Sie bilden eine multiplikative abelsche Gruppe, die der Gruppe der primen Restklassen modulo m isomorph ist. Das Einselement ist der Hauptcharakter χ_1 mit $\chi_1(a) = 1$ für $(a, m) = 1$. Es bestehen die Relationen

$$\sum_{n \bmod m} \chi(n) = \begin{cases} \varphi(m) & \text{für } \chi = \chi_1, \\ 0 & \text{für } \chi \neq \chi_1, \end{cases}$$

$$\sum_{\chi} \chi(n) = \begin{cases} \varphi(m) & \text{für } n \equiv 1 \quad (m), \\ 0 & \text{für } n \not\equiv 1 \quad (m). \end{cases}$$

Dabei wird die erste Summe über ein beliebiges vollständiges Restsystem modulo m und die zweite über alle Restklassencharaktere erstreckt.

Diesem allgemeinen Begriff des Restklassencharakters ordnet sich nun das in Kapitel 2 betrachtete *Legendre-Symbol* $\left(\frac{a}{p}\right)$, aufgefaßt als Funktion seines Zählers, unter. Es war für ungerade Primzahlen p und für alle ganzen Zahlen a mit $(a, p) = 1$ erklärt. Setzen wir zusätzlich $\left(\frac{a}{p}\right) = 0$ für $(a, p) > 1$, so erfüllt es alle Eigenschaften der Definition 3.5. Wegen $\left(\frac{a}{p}\right)^2 = 1$, $(a, p) = 1$, nennen wir es den *quadratischen Restklassencharakter* modulo p. Da für einen Charakter χ aus $\overline{\chi} = \chi^{-1}$ und der Forderung $\chi^2 = 1$ die Beziehung $\chi = \overline{\chi}$ entsteht, sind die quadratischen Restklassencharaktere modulo p als die vom Hauptcharakter verschiedenen *reellen Charaktere* festgelegt.

An dem Beispiel $m = 5$ soll noch die Bestimmung aller Restklassencharaktere modulo 5 demonstriert werden. Wegen $\varphi(5) = 4$ gibt es vier verschiedene Charaktere mit den möglichen Werten ± 1, $\pm i$ für $(a, 5) = 1$. Aus $\chi(2)\,\chi(3) = \chi(6) = \chi(1) = 1$ folgt $\chi(3) = \chi^{-1}(2)$. $\chi(4)$ ist durch $\chi(2)$ wegen $\chi(4) = \chi(2)^2$ festgelegt. Daraus erhält man die Tabelle

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

Insbesondere liest man $\chi_2(a) = \left(\frac{a}{5}\right)$ ab.

3.4. Gaußsche Summen

Definition 3.6. Es sei χ ein beliebiger Restklassencharakter modulo m. Die Summe

$$G(a, \chi) = \sum_{n \bmod m} \chi(n)\, e^{2\pi i \frac{an}{m}}$$

wird die zu χ gehörige *Gaußsche Summe* genannt. Dabei durchläuft n ein vollständiges Restsystem modulo m.

Es soll hier keine allgemeine Theorie der Gaußschen Summen entwickelt werden. Wir begnügen uns mit einigen wenigen Aussagen und legen unser Hauptaugenmerk auf die Gaußschen Summen nach quadratischen Restklassencharakteren. Beginnen wollen wir aber mit dem einfachsten Fall, der erst in Kapitel 5 von Bedeutung sein wird, nämlich der zum Hauptcharakter χ_1 gehörigen Gaußschen Summe. Diese wird auch *Ramanujansche Summe* genannt und üblicherweise durch $c_m(a) := G(a, \chi_1)$ bezeichnet. Es ist dann

$$c_m(a) = \sum_{\substack{n=1 \\ (n,m)=1}}^{m} e^{2\pi i \frac{an}{m}}.$$

Diese Summen lassen sich infolge ihrer Multiplikativität bezüglich m auf Primzahlpotenzen zurückführen und damit berechnen.

Satz 3.7. *Für* $(m_1, m_2) = 1$ ist

$$c_{m_1 m_2}(a) = c_{m_1}(a)\, c_{m_2}(a).$$

Für Primzahlen p *und* $\nu \geqq 1$ *gilt*

$$c_{p^\nu}(a) = \begin{cases} p^{\nu-1}(p-1) & \text{für } p^\nu \mid a, \\ -p^{\nu-1} & \text{für } p^{\nu-1} \mid a \wedge p^\nu \nmid a, \\ 0 & \text{für } p^{\nu-1} \nmid a. \end{cases}$$

Beweis. Durchlaufen n_j $(j = 1, 2)$ prime Restsysteme modulo m_j, so durchläuft $n_1 m_2 + n_2 m_1$ wegen $(m_1, m_2) = 1$ ein primes Restsystem modulo $m_1 m_2$. Daher ist

$$c_{m_1}(a)\, c_{m_2}(a) = \sum_{\substack{n_1=1 \\ (n_1,m_1)=1}}^{m_1} \sum_{\substack{n_2=1 \\ (n_2,m_2)=1}}^{m_2} e^{2\pi i a \frac{n_1 m_2 + n_2 m_1}{m_1 m_2}} = c_{m_1 m_2}(a).$$

Die angegebenen Werte für $c_{p^\nu}(a)$ ergeben sich sofort aus

$$c_{p^\nu}(a) = \sum_{\substack{n=1 \\ (n,p)=1}}^{p^\nu} e^{2\pi i a n p^{-\nu}} = \sum_{n=1}^{p^\nu} e^{2\pi i a n p^{-\nu}} - \sum_{n=1}^{p^{\nu-1}} e^{2\pi i a n p^{1-\nu}}.$$

Nun wenden wir uns einigen allgemeinen Aussagen über Gaußsche Summen zu.

Satz 3.8. *Für beliebigen Restklassencharakter* χ *modulo* m *und für* $(a, m) = 1$ *gilt*

$$G(a, \chi) = \overline{\chi(a)}\, G(1, \chi).$$

Beweis: Wegen $(a, m) = 1$ durchlaufen mit n auch die Zahlen an ein vollständiges Restsystem modulo m. Aus $\chi(a)\,\overline{\chi(a)} = 1$ folgt $\chi(n) = \overline{\chi(a)}\,\chi(a)\,\chi(n) = \overline{\chi(a)}\,\chi(an)$ und daher

$$G(a, \chi) = \sum_{n \bmod m} \chi(n)\, e^{2\pi i \frac{an}{m}} = \overline{\chi(a)} \sum_{n \bmod m} \chi(an)\, e^{2\pi i \frac{an}{m}}$$

$$= \overline{\chi(a)} \sum_{k \bmod m} \chi(k)\, e^{2\pi i \frac{k}{m}} = \overline{\chi(a)}\, G(1, \chi).$$

Ist $(a, m) > 1$, so ist stets $\chi(a) = 0$. Dagegen kann $G(a, \chi)$ sehr wohl von 0 verschieden sein. Der nächste Satz gibt eine notwendige Bedingung.

Satz 3.9. *Es sei χ ein Restklassencharakter modulo m. Für die ganze Zahl a sei $(a, m) > 1$ und $G(a, \chi) \neq 0$. Dann existiert ein Teiler t von m mit $0 < t < m$ und*

$$\chi(b) = 1 \quad \text{für} \quad (b, m) = 1 \wedge b \equiv 1 \quad (t).$$

Beweis. Es sei $(a, m) = d$ und $t = \dfrac{m}{d}$. Wegen $d > 1$ ist $0 < t < m$. Es sei b so gewählt, daß $(b, m) = 1$ und $b \equiv 1 \quad (t)$. Dann ist

$$G(a, \chi) = \sum_{n \bmod m} \chi(n)\, e^{2\pi i \frac{an}{m}} = \sum_{n \bmod m} \chi(bn)\, e^{2\pi i \frac{abn}{m}}$$

$$= \chi(b) \sum_{n \bmod m} \chi(n)\, e^{2\pi i \frac{abn}{m}}.$$

Aus $abn = an + antk = an + \dfrac{a}{d}\, nmk \equiv an \quad (m)$ ergibt sich

$$G(a, \chi) = \chi(b) \sum_{n \bmod m} \chi(n)\, e^{2\pi i \frac{an}{m}} = \chi(b)\, G(a, \chi).$$

Für $G(a, \chi) \neq 0$ muß dann notwendigerweise $\chi(b) = 1$ sein, was den Satz beweist.

Definition 3.7. Ein Restklassencharakter χ modulo m heißt *primitiv*, wenn es für jeden Teiler t von m, $0 < t < m$, eine ganze Zahl b mit $b \equiv 1 \quad (t)$, $(b, m) = 1$, gibt, so daß $\chi(b) \neq 1$ ist.

Für $m > 1$ ist der Hauptcharakter χ_1 nicht primitiv, da $\chi_1(b) = 1$ für alle b mit $(b, m) = 1$ ist.

Ist $m = p$ eine Primzahl, so ist jeder vom Hauptcharakter verschiedene Charakter χ primitiv. Der einzig mögliche Teiler t von p mit $0 < t < p$ ist $t = 1$. Wäre χ nicht primitiv, so müßte $\chi(b) = 1$ für alle b mit $(b, p) = 1$ sein. Das kann aber nur der Hauptcharakter sein.

Satz 3.10. *Ist χ ein primitiver Restklassencharakter modulo m, so ist $G(a, \chi) = 0$ für jedes a mit $(a, m) > 1$.*

Beweis. Gibt es ein a mit $G(a, \chi) \neq 0$ und $(a, m) > 1$, so gibt es nach Satz 3.9 einen Teiler t von m mit $0 < t < m$, so daß $\chi(b) = 1$ für $(b, m) = 1$ und $b \equiv 1 \pmod{t}$ wird. Dann kann aber χ nicht primitiv sein.

Satz 3.11. *Ist χ ein primitiver Restklassencharakter modulo m, so gilt*

$$|G(1, \chi)| = \sqrt{m}.$$

Beweis. Die Behauptung folgt aus

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

Im Hinblick auf das *quadratische Reziprozitätsgesetz* betrachten wir jetzt den *quadratischen Restklassencharakter* $\chi(a) = \left(\frac{a}{p}\right)$ nach einer ungeraden Primzahl p. Wir haben dann

$$G(a, \chi) = \sum_{n=1}^{p-1}\left(\frac{n}{p}\right)e^{2\pi i\frac{an}{p}}$$

und nach Satz 3.8

$$G(a, \chi) = \left(\frac{a}{p}\right)G(1, \chi).$$

Gegenüber Satz 3.11 können wir ein weitergehendes Resultat erzielen.

Satz 3.12. *Ist p eine ungerade Primzahl und $\chi(n) = \left(\frac{n}{p}\right)$, so gilt*

$$G(1, \chi)^2 = (-1)^{\frac{p-1}{2}}p. \tag{9}$$

Beweis. Es ist

$$G(1,\chi)^2 = \sum_{n=1}^{p-1}\sum_{k=1}^{p-1}\left(\frac{n}{p}\right)\left(\frac{k}{p}\right)e^{2\pi i\frac{n+k}{p}}.$$

Für festes n gibt es zu jedem k ein durch $k \equiv nm \pmod{p}$ eindeutig bestimmtes m mit $(m, p) = 1$. Daher ist

$$\begin{aligned}G(1,\chi)^2 &= \sum_{n=1}^{p-1}\sum_{m=1}^{p-1}\left(\frac{n^2m}{p}\right)e^{2\pi i\frac{n(m+1)}{p}} = \sum_{m=1}^{p-1}\left(\frac{m}{p}\right)\sum_{n=1}^{p-1}e^{2\pi i\frac{n(m+1)}{p}}\\ &= -\sum_{m=1}^{p-2}\left(\frac{m}{p}\right) + (p-1)\left(\frac{-1}{p}\right) = -\sum_{m=1}^{p-1}\left(\frac{m}{p}\right) + p\left(\frac{-1}{p}\right)\\ &= (-1)^{\frac{p-1}{2}}p\end{aligned}$$

nach den Sätzen 2.26 und 2.29.

Zur Berechnung von $G(1, \chi)$ für $\chi(n) = \left(\frac{n}{p}\right)$ ist nach (9) in

$$G(1, \chi) = \pm\sqrt{(-1)^{\frac{p-1}{2}} p}$$

„nur" noch das Vorzeichen zu bestimmen. Aber darin liegt die eigentliche ganze Schwierigkeit, die selbst C. F. Gauss erst nach mehreren vergeblichen Versuchen meistern konnte. Wir werden dieses Problem im nächsten Abschnitt lösen, befreien uns aber zunächst in der Definition dieser speziellen Gaußschen Summe von der direkten Verwendung des Restklassencharakters $\left(\frac{n}{p}\right)$. Für ungerade Primzahlen p ist nämlich

$$G(a, \chi) = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) e^{2\pi i \frac{ak}{p}} = \sum_{r} e^{2\pi i \frac{ar}{p}} - \sum_{n} e^{2\pi i \frac{an}{p}},$$

wobei in der ersten Summe über alle quadratischen Reste r und in der zweiten Summe über alle quadratischen Nicht-Reste n modulo p zu summieren ist. Aus

$$1 + \sum_{r} e^{2\pi i \frac{ar}{p}} + \sum_{n} e^{2\pi i \frac{an}{p}} = \sum_{k=0}^{p-1} e^{2\pi i \frac{ak}{p}} = 0$$

für $(a, p) = 1$ folgt

$$G(a, \chi) = 1 + 2\sum_{r} e^{2\pi i \frac{ar}{p}},$$

und da jede Kongruenz $x^2 \equiv r \pmod{p}$ genau zwei Lösungen $x \equiv \pm k \pmod{p}$ hat, erhalten wir

$$G(a, \chi) = \sum_{k=0}^{p-1} e^{2\pi i \frac{a}{p} k^2}. \tag{10}$$

3.5. Das quadratische Reziprozitätsgesetz im Lichte der Gaußschen Summen

Die Darstellung (10) soll zum Anlaß genommen werden, derartige Summen auch dann zu erklären, wenn p keine Primzahl ist.

Definition 3.8. Es sei a eine natürliche Zahl und b eine ganze Zahl mit $(a, b) = 1$. Die Summe

$$G_a(b) = \sum_{n=0}^{a-1} e^{2\pi i \frac{b}{a} n^2}$$

wird *quadratische Gaußsche Summe* genannt.

Unsere Aufgabe soll darin bestehen, diese Summe zu berechnen. Zunächst wird sich zeigen, daß die quadratische Gaußsche Summe bezüglich a einer multiplikativen Eigenschaft genügt. Damit können wir uns auf den Fall einer Primzahlpotenz $a = p^s$

beschränken. Für $p = 2$ gelingt uns sodann die Berechnung von $G_a(b)$ sofort. Für $a = 2^\nu$ berechnen wir vorerst nur $G_a(1)$. In Verbindung mit einem *Reziprozitätsgesetz*, welches $G_a(b)$ in $G_{|b|}(a)$ überführt, können wir schließlich $G_a(b)$ rekursiv berechnen. Über (10) gelingt uns dann eine Verbindung zum quadratischen Reziprozitätsgesetz.

Satz 3.13. *Für* $(a, a') = 1$ *gilt*

$$G_a(a'b)\, G_{a'}(ab) = G_{aa'}(b).$$

Beweis. Es ist

$$G_a(a'b)\, G_{a'}(ab) = \sum_{n=0}^{a-1} \sum_{n'=0}^{a'-1} e^{2\pi i \frac{b}{aa'}(a'^2 n^2 + a^2 n'^2)}$$

$$= \sum_{n=0}^{a-1} \sum_{n'=0}^{a'-1} e^{2\pi i \frac{b}{aa'}(a'n + an')^2}$$

$$= \sum_{k=0}^{aa'-1} e^{2\pi i \frac{b}{aa'} k^2} = G_{aa'}(b)$$

unter Ausnutzung des Hilfssatzes 2.1.

Satz 3.14. *Für* $b \equiv 1 \quad (2)$ *ist*

$$G_2(b) = 0 \tag{11}$$

und für $\nu > 1$

$$G_{2^\nu}(b) = \begin{cases} 2^{\nu/2}(1 + i^b) & \text{für } \nu \equiv 0 \quad (2), \\ 2^{\frac{\nu+1}{2}} e^{\pi i \frac{b}{4}} & \text{für } \nu \equiv 1 \quad (2). \end{cases} \tag{12}$$

Beweis. Durch Ausrechnen bestätigt man leicht (11) und für $\nu = 2,3$ auch (12). Setzen wir jetzt $\nu > 3$ voraus. Dann ist

$$G_{2^\nu}(b) = \sum_{n=0}^{2^{\nu-2}-1} \sum_{r=0}^{3} e^{2\pi i b 2^{-\nu}(n + 2^{\nu-2} r)^2}$$

$$= \sum_{n=0}^{2^{\nu-2}-1} e^{2\pi i b 2^{-\nu} n^2} \sum_{r=0}^{3} e^{\pi i b n r}$$

$$= 4 \sum_{m=0}^{2^{\nu-3}-1} e^{2\pi i b 2^{4-\nu} m^2},$$

da die Summe über r für ungerade n den Wert 0, für $n = 2m$ den Wert 4 annimmt. Wegen $(m + 2^{\nu-3})^2 \equiv m^2 \quad (2^{\nu-3})$ für $\nu > 3$ folgt

$$G_{2^\nu}(b) = 2 \sum_{m=0}^{2^{\nu-2}-1} e^{2\pi i b 2^{4-\nu} m^2} = 2 G_{2^{\nu-1}}(b).$$

Damit kann $G_{2^\nu}(b)$ auf $G_4(b)$ oder $G_8(b)$ zurückgeführt werden, je nachdem, ob ν gerade oder ungerade ist. Aus diesen Anfangswerten ergibt sich unmittelbar (12).

Die Berechnung des Betrages der quadratischen Gaußschen Summe bietet keinerlei Schwierigkeiten.

Satz 3.15. *Für* $(a, b) = 1$ *ist*

$$|G_a(b)| = \begin{cases} \sqrt{a} & \text{für} \quad a \equiv 1 \quad (2), \\ \sqrt{2a} & \text{für} \quad a \equiv 0 \quad (4), \\ 0 & \text{für} \quad a \equiv 2 \quad (4). \end{cases} \tag{13}$$

Beweis. Wir behandeln die drei Fälle getrennt.

1. $a \equiv 1 \quad (2)$:

$$|G_a(b)|^2 = \sum_{n_1=0}^{a-1} \sum_{n_2=0}^{a-1} e^{2\pi i \frac{b}{a}(n_1^2 - n_2^2)}.$$

Wir setzen $n_1 = n_2 + m$. Durchläuft n_1 bei festem n_2 ein vollständiges Restsystem modulo a, dann auch m. Daher ist

$$|G_a(b)|^2 = \sum_{m=0}^{a-1} e^{2\pi i \frac{b}{a} m^2} \sum_{n_2=0}^{a-1} e^{4\pi i \frac{b}{a} m n_2} = a, \tag{14}$$

da die Summe über n_2 für $m = 0$ den Wert a, sonst aber 0 hat.

2. $a \equiv 0 \quad (4)$: Wir können die Entwicklung (14) benutzen. Die Summe über n_2 hat jetzt für $m = 0$ und $m = \frac{a}{2}$ den Wert a, sonst 0. Daher ist $|G_a(b)|^2 = 2a$.

3. $a \equiv 2 \quad (4)$: Mit $a = 2u$, $u \equiv 1 \quad (2)$, folgt aus Satz 3.13 und (11)

$$G_a(b) = G_2(ub)\, G_u(2b) = 0.$$

Damit ist der Satz in allen Teilen bewiesen.

Wir nehmen jetzt die Berechnung von $G_a(1)$ über eine *Produktdarstellung der quadratischen Gaußschen Summe* vor. Diesem Ziel dienen die beiden folgenden Hilfssätze.

Hilfssatz 3.1. *Für ungerade, natürliche Zahlen* n *und beliebige reelle Zahlen* x *gilt*

$$\prod_{\nu=0}^{n-1} \sin 2\pi \left(x + \frac{\nu}{n} \right) = 2^{1-n} (-1)^{\frac{n-1}{2}} \sin 2\pi nx. \tag{15}$$

Insbesondere ist

$$\prod_{\nu=1}^{\frac{n-1}{2}} \sin 2\pi \frac{\nu}{n} = 2^{\frac{1-n}{2}} \sqrt{n}, \tag{16}$$

$$\prod_{\nu=1}^{\frac{n-1}{2}} \cos 2\pi \frac{\nu}{n} = (-1)^{\frac{n^2-1}{8}} 2^{\frac{1-n}{2}}. \tag{17}$$

Hier und in folgendem sollen leere Produkte stets den Wert 1 haben.

Beweis. Die Lösungen von $z^n - 1 = 0$, die n-ten Einheitswurzeln, sind gegeben durch

$$z_\nu = e^{2\pi i \frac{\nu}{n}} \qquad (\nu = 0, 1, \ldots, n-1).$$

Daher ist

$$\prod_{\nu=0}^{n-1} \left(z - e^{2\pi i \frac{\nu}{n}}\right) = z^n - 1.$$

Da n ungerade ist, durchläuft mit ν auch 2ν ein volles Restsystem modulo n. Setzen wir noch $z = e^{-4\pi i x}$, so haben wir

$$\prod_{\nu=0}^{n-1} \left(e^{-4\pi i x} - e^{2\pi i \frac{\nu}{n}}\right) = e^{-4\pi i n x} - 1.$$

Durch Multiplikation dieser Gleichung mit

$$\prod_{\nu=0}^{n-1} \left(-e^{2\pi i \left(x - \frac{\nu}{n}\right)}\right) = -e^{2\pi i n x}$$

ergibt sich

$$\prod_{\nu=0}^{n-1} \left(e^{2\pi i \left(x + \frac{\nu}{n}\right)} - e^{-2\pi i \left(x + \frac{\nu}{n}\right)}\right) = e^{2\pi i n x} - e^{-2\pi i n x}$$

und damit (15). Der Grenzübergang $x \to 0$ liefert aus

$$\prod_{\nu=1}^{n-1} \sin 2\pi \left(x + \frac{\nu}{n}\right) = 2^{1-n}(-1)^{\frac{n-1}{2}} \frac{\sin 2\pi n x}{\sin 2\pi x}$$

die Gleichung

$$\prod_{\nu=1}^{n-1} \sin 2\pi \frac{\nu}{n} = 2^{1-n}(-1)^{\frac{n-1}{2}} n.$$

Hieraus gewinnen wir

$$\prod_{\nu=1}^{\frac{n-1}{2}} \sin 2\pi \frac{\nu}{n} \sin 2\pi \frac{n-\nu}{n} = 2^{1-n}(-1)^{\frac{n-1}{2}} n,$$

$$\prod_{\nu=1}^{\frac{n-1}{2}} \sin^2 2\pi \frac{\nu}{n} = 2^{1-n} n.$$

Da $\sin 2\pi \frac{\nu}{n} > 0$ für $1 \leqq \nu \leqq \frac{n-1}{2}$ ist, folgt hieraus (16). Zum Nachweis von (17)

setzen wir in (15) $x = \frac{1}{4}$ und erhalten

$$\prod_{\nu=1}^{n-1} \cos 2\pi \frac{\nu}{n} = 2^{1-n},$$

$$\prod_{\nu=1}^{\frac{n-1}{2}} \cos^2 2\pi \frac{\nu}{n} = 2^{1-n},$$

$$\prod_{\nu=1}^{\frac{n-1}{2}} \cos 2\pi \frac{\nu}{n} = \pm 2^{\frac{1-n}{2}}.$$

Zur Bestimmung des Vorzeichens stellen wir $\cos 2\pi \frac{\nu}{n} > 0$ für $1 \leqq \nu < \frac{n}{4}$ und $\cos 2\pi \frac{\nu}{n} < 0$ für $\frac{n}{4} < \nu \leqq \frac{n-1}{2}$ fest. In den Faktoren des Produktes (17) tritt also $\frac{n-1}{2} - \left[\frac{n}{4}\right]$-mal das Minuszeichen auf. Durch eine leichte Rechnung bestätigt man $\frac{n-1}{2} - \left[\frac{n}{4}\right] \equiv \frac{n^2-1}{8}$ (2). Damit ist auch (17) bewiesen.

Hilfssatz 3.2. *Mit* $c_0(x, n) = 1$ *und*

$$c_\nu(x, n) = \prod_{k=1}^{\nu} \frac{1 - x^{n-k+1}}{1 - x^k} \qquad (\nu = 1, 2, \ldots, n)$$

gilt für nichtnegative ganze Zahlen n *mit* $n \equiv 0$ (2)

$$\sum_{\nu=0}^{n} (-1)^\nu c_\nu(x, n) = \prod_{k=1}^{n/2} (1 - x^{2k-1}). \tag{18}$$

Beweis. Für $n = 0$ ist die Gültigkeit von (18) trivial. Wir betrachten die linke Seite von (18) zunächst für beliebige ganze Zahlen $n \geqq 2$. Aus der Definition von $c_\nu(x, n)$ folgt

$$c_\nu(x, n) = \frac{1 - x^n}{1 - x^{n-\nu}} c_\nu(x, n-1) = c_\nu(x, n-1) + x^{n-\nu} \frac{1 - x^\nu}{1 - x^{n-\nu}} c_\nu(x, n-1)$$

$$= c_\nu(x, n-1) + x^{n-\nu} c_{\nu-1}(x, n-1).$$

Daher ist, wenn wir die linke Seite von (18) mit $f(x, n)$ bezeichnen,

$$f(x, n) = 1 + (-1)^n + \sum_{\nu=1}^{n-1} (-1)^\nu c_\nu(x, n)$$

$$= 1 + (-1)^n + \sum_{\nu=1}^{n-1} (-1)^\nu \{c_\nu(x, n-1) + x^{n-\nu} c_{\nu-1}(x, n-1)\}$$

$$= \sum_{\nu=1}^{n-1} (-1)^{\nu-1} (1 - x^{n-\nu}) c_{\nu-1}(x, n-1)$$

$$= (1 - x^{n-1}) \sum_{\nu=1}^{n-1} (-1)^{\nu-1} c_{\nu-1}(x, n-2) = (1 - x^{n-1}) f(x, n-2).$$

Aus dieser Rekursionsformel folgt wegen $f(x, 1) = 0$ als Nebenergebnis $f(x, n) = 0$ für ungerade n und wegen $f(x, 0) = 1$ für gerade n die Behauptung (18).

Aus diesen beiden Hilfssätzen ergibt sich für die quadratische Gaußsche Summe eine Produktdarstellung, die eine Berechnung von $G_a(1)$ ermöglichen wird.

Satz 3.16. *Für* $(a, b) = 1$, $a \equiv 1 \pmod 2$ *gilt*

$$G_a(b) = 2^{\frac{a-1}{2}} \frac{1+i}{2} (1 + i^{-a}) \prod_{\nu=1}^{\frac{a-1}{2}} \sin 2\pi\nu \frac{b}{a}. \tag{19}$$

Beweis. Wir benutzen die Beziehung (18) mit $n = a - 1$ und $x = e^{-4\pi i \frac{b}{a}}$. Für $c_\nu(x, a-1)$ erhalten wir

$$c_\nu(x, a-1) = \prod_{k=1}^{\nu} \frac{1 - e^{4\pi i \frac{kb}{a}}}{1 - e^{-4\pi i \frac{kb}{a}}} = (-1)^\nu e^{2\pi i \nu(\nu+1)\frac{b}{a}}$$

und damit für die linke Seite von (18)

$$\sum_{\nu=0}^{a-1} (-1)^\nu c_\nu(x, a-1) = \sum_{\nu=0}^{a-1} e^{2\pi i \nu(\nu+1)\frac{b}{a}} = e^{-2\pi i \left(\frac{a-1}{2}\right)^2 \frac{b}{a}} \sum_{\nu=0}^{a-1} e^{2\pi i \left(\frac{a-1}{2} - \nu\right)^2 \frac{b}{a}}$$

$$= e^{-2\pi i \left(\frac{a-1}{2}\right)^2 \frac{b}{a}} G_a(b). \tag{20}$$

Für die rechte Seite von (18) erhalten wir

$$\prod_{k=1}^{\frac{a-1}{2}} (1 - x^{2k-1}) = \prod_{k=1}^{\frac{a-1}{2}} \left(1 - e^{-4\pi i (2k-1)\frac{b}{a}}\right)$$

$$= e^{-2\pi i \left(\frac{a-1}{2}\right)^2 \frac{b}{a}} (2i)^{\frac{a-1}{2}} \prod_{k=1}^{\frac{a-1}{2}} \sin 2\pi(2k-1)\frac{b}{a}. \tag{21}$$

Zur Umformung des Produktes auf die Gestalt (19) unterscheiden wir die Fälle $a \equiv 1 \pmod 4$ (4) und $a \equiv 3 \pmod 4$ (4). Im Fall $a \equiv 1 \pmod 4$ (4) bilden die Zahlen $2k - 1$ für $1 \leqq k \leqq \frac{a-1}{4}$ die ungeraden Zahlen unterhalb $\frac{a-1}{2}$. Für $\frac{a+3}{4} \leqq k \leqq \frac{a-1}{2}$ ist $\sin 2\pi(2k-1)\frac{b}{a} = \sin 2\pi(a - 2k')\frac{b}{a} = -\sin 2\pi 2k'\frac{b}{a}$ mit $k' = \frac{a+1}{2} - k$. Dadurch erhalten wir ergänzend die geraden Zahlen $2k'$ unterhalb $\frac{a-1}{2}$. Hinzu kommen $\frac{a-1}{4}$ Minuszeichen. Aus (21) entsteht

$$\prod_{k=1}^{\frac{a-1}{2}} (1 - x^{2k-1}) = e^{-2\pi i \left(\frac{a-1}{2}\right)^2 \frac{b}{a}} 2^{\frac{a-1}{2}} \prod_{\nu=1}^{\frac{a-1}{2}} \sin 2\pi\nu\frac{b}{a}. \tag{22}$$

Analog bilden im Fall $a \equiv 3$ (4) die Zahlen $2k-1$ für $1 \leqq k \leqq \frac{a+1}{4}$ die ungeraden Zahlen unterhalb $\frac{a-1}{2}$. Für $\frac{a+5}{4} \leqq k \leqq \frac{a-1}{2}$ ist $\sin 2\pi(2k-1)\frac{b}{a}$ $= -\sin 2\pi 2k'\frac{b}{a}$ mit $k' = \frac{a+1}{2} - k$. Wir erhalten die ergänzenden geraden Zahlen $2k'$ verbunden mit $\frac{a-3}{4}$ Minuszeichen. Aus (21) wird

$$\prod_{k=1}^{\frac{a-1}{2}} (1 - x^{2k-1}) = e^{-2\pi i\left(\frac{a-1}{2}\right)^2\frac{b}{a}}\, i^{\frac{a-1}{2}} \prod_{\nu=1}^{\frac{a-1}{2}} \sin 2\pi\nu\frac{b}{a}. \tag{23}$$

(18) liefert die Identität einerseits von (20) und (22) und andererseits von (20) und (23). Beide Identitäten zusammengefaßt ergeben (19).

Satz 3.17 (Gauss).

$$G_a(1) = \frac{1+i}{2}(1 + i^{-a})\sqrt{a}. \tag{24}$$

Beweis. Für $a \equiv 2$ (4) folgt (24) aus (13). Auch für $a \equiv 1$ (2) ergibt sich (24) sofort aus (16) und (19). Für $a \equiv 0$ (4) setzen wir $a = 2^\alpha u$ mit $\alpha \geqq 2$, $u \equiv 1$ (2). Damit erhalten wir aus Satz 3.13

$$G_a(1) = G_{2^\alpha}(u)\, G_u(2^\alpha).$$

Ist α gerade, so ist $G_u(2^\alpha) = G_u(1)$. Hierfür ist (24) schon bewiesen, und mit (12) ist

$$G_a(1) = 2^{\alpha/2}(1 + i^u)\frac{1+i}{2}(1 + i^{-u})\sqrt{u} = (1+i)\sqrt{a}.$$

Ist α ungerade, so ist $G_u(2^\alpha) = G_u(2)$. Hier folgt aus (19)

$$G_u(2^\alpha) = 2^{\frac{u-1}{2}}\frac{1+i}{2}(1 + i^{-u})\prod_{\nu=1}^{\frac{u-1}{2}} \sin\frac{4\pi\nu}{u}$$

$$= 2^{u-2}(1+i)(1 + i^{-u})\prod_{\nu=1}^{\frac{u-1}{2}} \sin\frac{2\pi\nu}{u}\cos\frac{2\pi\nu}{u}$$

und aus (16), (17)

$$G_u(2^\alpha) = (-1)^{\frac{u^2-1}{8}}\frac{1+i}{2}(1 + i^{-u})\sqrt{u}.$$

Damit ergibt sich aus (12)

$$G_a(1) = (-1)^{\frac{u^2-1}{8}}\frac{1+i}{\sqrt{2}}(1 + i^{-u})\, e^{\pi i\frac{u}{4}}\sqrt{a} = (1+i)\sqrt{a},$$

und der Satz ist in allen Teilen bewiesen.

Nunmehr sind wir in der Lage, für die quadratischen Gaußschen Summen selbst ein Reziprozitätsgesetz aufzustellen, aus dem das quadratische Reziprozitätsgesetz unmittelbar folgt.

Satz 3.18. *Sind a, b natürliche Zahlen mit $(a, b) = 1$, und ist $b \equiv 1 \pmod 2$, so gilt*

$$G_a(b) = \sqrt{\frac{a}{b}} \frac{1+i}{2} (1 + i^{-ab}) \overline{G_b(a)}. \tag{25}$$

Beweis. Nach Satz 3.13 ist für $(a, b) = 1$

$$G_a(b)\, G_b(a) = G_{ab}(1).$$

Durch Multiplikation mit dem Konjugiertkomplexen von $G_b(a)$ erhält man

$$G_a(b)\, |G_b(a)|^2 = G_{ab}(1)\, \overline{G_b(a)}.$$

Nach (13) ist $|G_b(a)|^2 = b$ für $b \equiv 1 \pmod 2$. Setzt man dies und für $G_{ab}(1)$ noch (24) ein, so ergibt sich (25).

Anwendung auf die quadratischen Reste: Ist p eine ungerade Primzahl und q eine beliebige Zahl mit $(p, q) = 1$, so ist nach Satz 3.8, (10), und Definition 3.8

$$G_p(q) = \left(\frac{q}{p}\right) G_p(1).$$

Durch Eintragen von (19) findet man daraus die merkwürdige *Darstellung des Legendre-Symbols*

$$\left(\frac{q}{p}\right) = \prod_{\nu=1}^{\frac{p-1}{2}} \frac{\sin 2\pi\nu \frac{q}{p}}{\sin 2\pi\nu \frac{1}{p}} \tag{26}$$

oder mit (16)

$$\left(\frac{q}{p}\right) = \frac{2^{\frac{p-1}{2}}}{\sqrt{p}} \prod_{\nu=1}^{\frac{p-1}{2}} \sin 2\pi\nu \frac{q}{p}. \tag{27}$$

Die beiden Ergänzungssätze des quadratischen Reziprozitätsgesetzes

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

liest man aus (27) bei Verwendung von (16) und (17) mühelos ab.

Für den Beweis des quadratischen Reziprozitätsgesetzes bieten sich jetzt zwei Varianten an: Entweder man benutzt die Produktdarstellung (26) des Legendre-Symbols oder direkt das Reziprozitätsgesetz (25) der Gaußschen Summen. Da beide Beweise nach der geleisteten Hauptarbeit sehr kurz sind, sollen auch beide dargestellt werden. Dabei bedeuten p, q jetzt immer ungerade Primzahlen mit $p \neq q$.

1. Variante: *Benutzung der Produktdarstellung* (26) *des Legendre-Symbols.* Hierzu sei nebenbei bemerkt, daß die Darstellung (26) allein aus dem Eulerschen Kriterium und dem Hilfssatz 3.1 gewonnen werden kann, so daß der hier eingeschlagene Weg über die Gaußschen Summen völlig unnötig ist. Nach (15) ist

$$\frac{\sin 2\pi\nu\,\frac{q}{p}}{\sin 2\pi\nu\,\frac{1}{p}} = 2^{q-1}(-1)^{\frac{q-1}{2}}\prod_{\nu'=1}^{q-1}\sin 2\pi\left(\frac{\nu}{p}+\frac{\nu'}{q}\right)$$

$$= (-4)^{\frac{q-1}{2}}\prod_{\nu'=1}^{\frac{q-1}{2}}\sin 2\pi\left(\frac{\nu}{p}+\frac{\nu'}{q}\right)\sin 2\pi\left(\frac{\nu}{p}-\frac{\nu'}{q}\right).$$

Durch Einsetzen in (26) erhält man

$$\left(\frac{q}{p}\right) = (-4)^{\frac{(p-1)(q-1)}{4}}\prod_{\nu=1}^{\frac{p-1}{2}}\prod_{\nu'=1}^{\frac{q-1}{2}}\sin 2\pi\left(\frac{\nu}{p}+\frac{\nu'}{q}\right)\sin 2\pi\left(\frac{\nu}{p}-\frac{\nu'}{q}\right)$$

und bei Vertauschung von p und q das quadratische Reziprozitätsgesetz

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

2. Variante: *Benutzung des Reziprozitätsgesetzes* (25) *der Gaußschen Summen.* Aus $G_p(q) = \left(\frac{q}{p}\right) G_p(1)$ und aus (24) leitet sich wegen der Ungeradheit von p

$$G_p(q) = \left(\frac{q}{p}\right) i^{\left(\frac{p-1}{2}\right)^2}\sqrt{p}$$

und ebenso

$$G_q(p) = \left(\frac{p}{q}\right) i^{\frac{(q-1)^2}{2}}\sqrt{q}$$

her. (25) läßt sich auf die Gestalt

$$G_p(q) = \sqrt{\frac{p}{q}}\, i^{\left(\frac{pq-1}{2}\right)^2}\overline{G_q(p)}$$

bringen. Durch Einsetzen erhält man

$$\left(\frac{q}{p}\right) = i^{\left(\frac{pq-1}{2}\right)^2-\left(\frac{p-1}{2}\right)^2-\left(\frac{q-1}{2}\right)^2}\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

3.6. Aufgaben

1. Man bestimme das Produkt sämtlicher Elemente einer endlichen abelschen Gruppe.
2. Es sind alle abelschen Gruppen der Ordnung 6, 18, 30 und ihre Zerlegungen in direkte Produkte zyklischer Gruppen anzugeben.
3. Man bestimme sämtliche abelschen Gruppen der Ordnung 8 und gebe für jede Gruppe die zugehörigen Charaktere an.
4. Es seien p eine ungerade Primzahl, $p \nmid b$ und $\nu \geqq 2$. Man zeige

$$G_{p^\nu}(b) = pG_{p^{\nu-1}}(b)$$

und schließe daraus

$$G_{p^\nu}(b) = \begin{cases} p^{\nu/2} & \text{für } \nu \equiv 0 \quad (2), \\ p^{\frac{\nu-1}{2}} G_p(b) & \text{für } \nu \equiv 1 \quad (2). \end{cases}$$

5. Es sei p eine ungerade Primzahl, $p \nmid b$ und $\nu \equiv 1 \quad (2)$. Man beweise

$$G_{p^\nu}(b) = \begin{cases} \left(\frac{b}{p}\right) p^{\nu/2} & \text{für } p \equiv 1 \quad (4), \\ i\left(\frac{b}{p}\right) p^{\nu/2} & \text{für } p \equiv 3 \quad (4). \end{cases}$$

4. Algebraische und transzendente Zahlen

Die bekannten systematischen Bruchentwicklungen der reellen Zahlen vermögen nur höchst unvollkommen die Eigenschaften der durch sie dargestellten Zahlen widerzuspiegeln. Jede derartige Entwicklung vermittelt im wesentlichen nur einen Zusammenhang zwischen der betreffenden Zahl und der gewählten Grundzahl, bei der Dezimalbruchentwicklung der Grundzahl 10. Selbst die Unterscheidung zwischen den rationalen und irrationalen Zahlen ist verhältnismäßig kompliziert. In diesem Kapitel werden wir Darstellungen der reellen Zahlen — die Kettenbruchentwicklungen — kennenlernen, die unabhängig von besonders ausgewählten Zahlen sind. Die rationalen werden von den irrationalen Zahlen in einfacher Weise durch die Endlichkeit beziehungsweise Unendlichkeit der Entwicklungen getrennt. Darüber hinaus liefern die an einer Stelle abgebrochenen Entwicklungen in einem gewissen Sinne beste Approximationen durch rationale Zahlen. Wir setzen die Untersuchungen der irrationalen Zahlen durch ihre Unterscheidung in algebraische und transzendente Zahlen fort. Es wird sich herausstellen, daß „fast alle" Zahlen transzendent sind. Das Kapitel wird mit dem Nachweis der Transzendenz der Zahlen e und π abgeschlossen.

4.1. Die Entwicklung reeller Zahlen in Kettenbrüche

Der in 1.3 entwickelte *Euklidische Algorithmus* zur Bestimmung des größten gemeinsamen Teilers zweier natürlicher Zahlen kann andererseits zur Entwicklung von rationalen Zahlen in Kettenbrüche ausgenutzt werden. Sind $a_0, a_1 \in \mathbf{N}$ mit $a_0 > a_1 > 1$, so folgt aus dem Euklidischen Schema in 1.3

$$\frac{a_0}{a_1} = q_1 + \frac{a_2}{a_1} \qquad 0 < \frac{a_2}{a_1} < 1$$

$$\frac{a_1}{a_2} = q_2 + \frac{a_3}{a_2} \qquad 0 < \frac{a_3}{a_2} < 1$$

$$\cdots\cdots\cdots \qquad \cdots\cdots\cdots$$

$$\frac{a_{n-2}}{a_{n-1}} = q_{n-1} + \frac{a_n}{a_{n-1}} \qquad 0 < \frac{a_n}{a_{n-1}} < 1$$

$$\frac{a_{n-1}}{a_n} = q_n \qquad (0 = a_{n+1}).$$

Trägt man nacheinander die 2., 3., ..., n-te Gleichung in die erste Gleichung ein, so erhält man für a_0/a_1 die Entwicklung

$$\frac{a_0}{a_1} = q_1 + \cfrac{1}{q_2 + \cfrac{a_3}{a_2}} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{a_4}{a_3}}}$$

$$\vdots$$

$$= q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}.$$

Diese Entwicklung nehmen wir zum Anlaß, allgemein den Begriff eines Kettenbruches festzulegen.

Definition 4.1. Unter einem *Kettenbruch* versteht man die Entwicklung

$$[a_0; a_1, a_2, \ldots] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}}.$$

Dabei ist a_0 eine beliebige relle Zahl, und die Teilnenner $a_1, a_2, \ldots$ sind positive Zahlen.

Ist die Folge $\{a_n\}$ eine unendliche Folge reeller Zahlen, so spricht man von einem unendlichen Kettenbruch. Die gegebene Definition ist in diesem Fall zunächst ganz formal, da noch die Frage der Konvergenz zu klären ist. Besteht die Folge $\{a_n\}$ nur aus endlich vielen Elementen, so haben wir einen endlichen Kettenbruch

$$[a_0; a_1, a_2, \ldots, a_m] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_m}}}.$$

Wir wollen unter $[a_0; a_1, a_2, \ldots, a_k]$ für $k \geqq 0$ den k-ten *Abschnitt* eines vorgelegten Kettenbruches $[a_0; a_1, a_2, \ldots]$ beziehungsweise $[a_0; a_1, a_2, \ldots, a_m]$ verstehen. Für den unendlichen Kettenbruch kann k beliebig, für den endlichen Kettenbruch muß $k \leqq m$ sein. Wir beschäftigen uns zunächst mit diesen Abschnitten.

Satz 4.1. *Die Zahlen* p_k und q_k *seien definiert durch*

$$p_{-1} = 1, \quad p_0 = a_0, \quad p_k = a_k p_{k-1} + p_{k-2} \qquad (k \geqq 1), \tag{1}$$

$$q_{-1} = 0, \quad q_0 = 1, \quad q_k = a_k q_{k-1} + q_{k-2} \qquad (k \geqq 1). \tag{2}$$

Dann läßt sich jeder k-te Abschnitt eines Kettenbruches $[a_0; a_1, a_2, \ldots]$ *darstellen in der Form*

$$[a_0; a_1, a_2, \ldots, a_k] = \frac{p_k}{q_k} \qquad (k \geqq 0). \tag{3}$$

Die Brüche p_k/q_k heißen die *Näherungsbrüche* k-ter Ordnung des vorgelegten Kettenbruches.

Beweis. Für $k = 0$ ist

$$[a_0] = a_0 = \frac{p_0}{q_0}$$

und für $k = 1$

$$[a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}.$$

Weiter schließen wir durch Induktion. Es sei die Darstellung (3) richtig für $k \leqq n$. Dann folgt die Richtigkeit für $n + 1$ über

$$[a_0; a_1, a_2, \ldots, a_n, a_{n+1}] = \left[a_0; a_1, a_2, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}\right]$$

$$= \frac{\left(a_n + \frac{1}{a_{n+1}}\right) p_{n-1} + p_{n-2}}{\left(a_n + \frac{1}{a_{n+1}}\right) q_{n-1} + q_{n-2}} = \frac{a_{n+1}(a_n p_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1}(a_n q_{n-1} + q_{n-2}) + q_{n-1}}$$

$$= \frac{a_{n+1} p_n + p_{n-1}}{a_{n+1} q_n + q_{n-1}} = \frac{p_{n+1}}{q_{n+1}}.$$

Satz 4.2. *Für $k \geqq 0$ ist*

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}, \tag{4}$$

und für $k \geqq 1$ gilt

$$q_k p_{k-2} - p_k q_{k-2} = (-1)^{k-1} a_k. \tag{5}$$

Beweis. Durch Multiplikation der Rekursionsformeln (1), (2) mit q_{k-1} beziehungsweise p_{k-1} erhalten wir

$$p_k q_{k-1} = a_k p_{k-1} q_{k-1} + p_{k-2} q_{k-1},$$

$$p_{k-1} q_k = a_k p_{k-1} q_{k-1} + p_{k-1} q_{k-2}$$

und durch Subtraktion beider Gleichungen

$$p_k q_{k-1} - p_{k-1} q_k = -(p_{k-1} q_{k-2} - p_{k-2} q_{k-1})$$

$$= (-1)^k (p_0 q_{-1} - p_{-1} q_0) = (-1)^{k-1}.$$

Damit ist (4) bewiesen. Entsprechend ergibt sich aus (1), (2) durch Multiplikation mit q_{k-2} beziehungsweise p_{k-2}

$$q_k p_{k-2} = a_k q_{k-1} p_{k-2} + q_{k-2} p_{k-2},$$

$$p_k q_{k-2} = a_k p_{k-1} q_{k-2} + p_{k-2} q_{k-2}$$

und durch Subtraktion

$$q_k p_{k-2} - p_k q_{k-2} = -a_k(p_{k-1}q_{k-2} - q_{k-1}p_{k-2}).$$

Verwendet man hierin (4), so ergibt sich sofort (5).

Aus diesem Satz können wir eine wichtige Folgerung ziehen. Aus (5) folgt für $k \geqq 2$

$$\frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{(-1)^k a_k}{q_k q_{k-2}}.$$

Die rechte Seite dieser Gleichung ist für gerades k stets positiv und für ungerades k stets negativ. Also bilden die Näherungsbrüche gerader Ordnung eine streng monoton wachsende Folge, die Näherungsbrüche ungerader Ordnung eine streng monoton fallende Folge. Aus (4) ergibt sich für $k \geqq 1$

$$\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k-1}}{q_k q_{k-1}}.$$

Hieraus erkennt man, daß jeder Näherungsbruch ungerader Ordnung größer ist als jeder Näherungsbruch gerader Ordnung.

Insgesamt erhält man: Läßt sich die reelle Zahl α durch einen endlichen Kettenbruch $\alpha = [a_0; a_1, a_2, \ldots, a_n]$ darstellen, so ist für $2k + 1 < n$

$$\frac{p_{2k}}{q_{2k}} < \alpha < \frac{p_{2k+1}}{q_{2k+1}} \tag{6}$$

und $\alpha = \frac{p_n}{q_n}$. Jedem unendlichen Kettenbruch $[a_0; a_1, a_2, \ldots]$ entspricht eine Folge $\{p_k/q_k\}$ von Näherungsbrüchen. Konvergiert diese Folge, das heißt, ist $\lim\limits_{k\to\infty} p_k/q_k = \alpha$, so faßt man α als den Wert des unendlichen Kettenbruches auf und setzt $\alpha = [a_0; a_1, a_2, \ldots]$. Für die Folge der Näherungsbrüche gilt dann stets die Ungleichung (6).

Im weiteren wollen wir uns ausschließlich auf *Kettenbrüche mit natürlichen Elementen* beschränken. Dabei soll angenommen werden, daß die Zahlen $a_1, a_2, \ldots$ natürliche Zahlen sind und die Zahl a_0 ganz ist. Endliche Kettenbrüche mit letztem Element 1 sollen ausgeschlossen sein.

Satz 4.3. *Unendliche Kettenbrüche mit natürlichen Elementen sind stets konvergent.*

Beweis. Wir zeigen, daß die Folge $\{p_k/q_k\}$ dem Cauchyschen Konvergenzkriterium genügt: Zu jedem beliebigen $\varepsilon > 0$ gibt es eine natürliche Zahl n_0, so daß für alle $k, m > n_0$ gilt $\left|\frac{p_k}{q_k} - \frac{p_m}{q_m}\right| < \varepsilon$. Wir können $k > m$ annehmen. Dann ist

$$\left|\frac{p_k}{q_k} - \frac{p_m}{q_m}\right| \leqq \sum_{\nu=m}^{k-1} \left|\frac{p_{\nu+1}}{q_{\nu+1}} - \frac{p_\nu}{q_\nu}\right| = \sum_{\nu=m}^{k-1} \frac{1}{q_{\nu+1}q_\nu}.$$

Da $a_1, a_2, \ldots \in \mathbf{N}$ sind, folgt aus (2) $q_1 = a_1 \geqq 1$ und $q_k \geqq q_{k-1} + 1$ für $k \geqq 2$. Daher ist $q_k \geqq k$. Für unsere Abschätzung erhalten wir

$$\left|\frac{p_k}{q_k} - \frac{p_m}{q_m}\right| \leqq \sum_{\nu=m}^{k-1} \frac{1}{(\nu+1)\,\nu} = \sum_{\nu=m}^{k-1} \left(\frac{1}{\nu} - \frac{1}{\nu+1}\right) = \frac{1}{m} - \frac{1}{k}$$

$$< \frac{1}{m} < \frac{1}{n_0} < \varepsilon,$$

sofern man nur $n_0 > \frac{1}{\varepsilon}$ wählt. Dies beweist den Satz.

Satz 4.4. *Jede reelle Zahl α läßt sich eindeutig in einen Kettenbruch mit natürlichen Elementen entwickeln. Der zugehörige Kettenbruch ist endlich, wenn α rational ist; er ist unendlich, wenn α irrational ist.*

Beweis. Es bezeichne allgemein $[x]$ die größte ganze Zahl, die kleiner oder gleich x ist. Wir setzen

$$[\alpha] = a_0, \qquad \alpha = a_0 + \frac{1}{r_1}, \qquad \alpha = [a_0; r_1].$$

Dabei ist für nicht-ganzzahliges α stets $r_1 > 1$. Jetzt schreiben wir

$$[r_1] = a_1, \qquad r_1 = a_1 + \frac{1}{r_2}, \qquad \alpha = [a_0; a_1, r_2].$$

Diesen Prozeß setzen wir beliebig fort. Ist im n-ten Schritt $r_n > 1$, so bilden wir

$$[r_n] = a_n, \qquad r_n = a_n + \frac{1}{r_{n+1}}, \qquad \alpha = [a_0; a_1, \ldots, a_n, r_{n+1}]$$

mit $r_{n+1} > 1$. Diese Entwicklung gilt allgemein, sofern $r_1, r_2, \ldots, r_n$ nicht ganzzahlig sind.

Ist α rational, so sind auch alle r_n rational. Es zeigt sich, daß dann unser Prozeß nach endlich vielen Schritten abbricht. Ist nämlich $r_n = s_n/t_n$ mit natürlichen Zahlen s_n, t_n und $t_n > 1$, $(s_n, t_n) = 1$, so folgt aus

$$0 \leqq r_n - a_n = \frac{1}{r_{n+1}} < 1$$

$$0 \leqq \frac{s_n}{t_n} - a_n = \frac{s_n - a_n t_n}{t_n} = \frac{z_n}{t_n} < 1.$$

Damit ist $z_n < t_n$. Für $z_n = 0$ ist die Entwicklung beendet. Für $z_n > 0$ ist $r_{n+1} = t_n/z_n$. Damit hat r_{n+1} einen kleineren Nenner als r_n, weshalb die Folge $\{r_n\}$ nach endlich vielen Schritten eine natürliche Zahl erreicht. Die vorgegebene reelle Zahl α besitzt daher eine endliche Kettenbruchentwicklung, deren letztes Element größer als 1 ist.

Ist α irrational, so sind auch sämtliche r_n irrational, und der Prozeß läßt sich unbegrenzt fortsetzen. Dabei gilt für jedes n

$$\alpha = [a_0; a_1, \ldots, a_n; r_{n+1}],$$

$$\frac{p_n}{q_n} = [a_0; a_1, \ldots, a_n].$$

Wir zeigen, daß die Folge $\{p_n/q_n\}$ gegen α strebt. Es ist

$$\alpha - \frac{p_n}{q_n} = \frac{r_{n+1}p_n + p_{n-1}}{r_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{p_{n-1}q_n - p_nq_{n-1}}{q_n(r_{n+1}q_n + q_{n-1})}.$$

Mit Hilfe von (4) ergibt sich

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n(r_{n+1}q_n + q_{n-1})} < \frac{1}{q_n(a_{n+1}q_n + q_{n-1})} = \frac{1}{q_nq_{n+1}}. \tag{7}$$

Wegen $q_n \to \infty$ für $n \to \infty$ folgt daraus

$$\alpha = \lim_{n\to\infty} \frac{p_n}{q_n}.$$

Wir haben noch die Eindeutigkeit der Entwicklung nachzuweisen. Dazu nehmen wir an, α habe die beiden Entwicklungen

$$\alpha = [a_0; a_1, a_2, \ldots] = [a_0'; a_1', a_2', \ldots],$$

wobei die Kettenbrüche sowohl endlich als auch unendlich sein können. Offensichtlich ist $[x] = a_0 = a_0'$. Nun sei schon $a_k = a_k'$ für $k \leqq n$ nachgewiesen. Für diese k ist dann auch $p_k = p_k'$, $q_k = q_k'$, wenn p_k, q_k dem ersten und p_k', q_k' dem zweiten Kettenbruch zugeordnet sind. Aus

$$\alpha = \frac{r_{n+1}p_n + p_{n-1}}{r_{n+1}q_n + q_{n-1}} = \frac{r'_{n+1}p_n' + p'_{n-1}}{r'_{n+1}q_n' + q'_{n-1}} = \frac{r'_{n+1}p_n + p_{n-1}}{r'_{n+1}q_n + q_{n-1}}$$

folgt $r_{n+1} = r'_{n+1}$. Da $a_{n+1} = [r_{n+1}]$ und $a'_{n+1} = [r'_{n+1}]$ gilt, haben wir auch $a_{n+1} = a'_{n+1}$. So ist durch Induktion die Identität beider Kettenbrüche nachgewiesen, und der Satz ist in allen Teilen bewiesen.

Die Entwicklung der reellen Zahlen in Kettenbrüche mit natürlichen Elementen gibt gegenüber den systematischen Bruchentwicklungen nicht nur den Vorzug der scharfen Trennung der rationalen von den irrationalen Zahlen. Bricht man beide Entwicklungen an einer bestimmten Stelle ab, so erhält man *Approximationen* der vorgegebenen Zahl *durch rationale Zahlen*. Die durch die Näherungsbrüche der Kettenbruchentwicklung gegebenen Approximationen sind dabei erheblich besser. Dies zeigt die Ungleichung (7), die offensichtlich auch für endliche Entwicklungen zutrifft. Mit $q_{n+1} \geqq q_n$ folgt:

Satz 4.5. *Ist p_n/q_n der n-te Näherungsbruch der Kettenbruchentwicklung von α, so gilt*

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}.$$

Auf solche Approximationen von reellen Zahlen durch die Näherungsbrüche ihrer Kettenbruchentwicklung soll im nächsten Abschnitt noch näher eingegangen werden.

Wir betrachten hier noch *periodische Kettenbrüche*, die, wie sich zeigen wird, den *quadratischen Irrationalitäten* zugeordnet sind. Was versteht man unter einer quadratischen Irrationalität? Bekanntlich ist jede Zahl $\sqrt{N}$ irrational, wenn N eine natürliche Zahl darstellt, die keine Quadratzahl ist. Dabei ist $\sqrt{N}$ Lösung der Gleichung $x^2 - N = 0$. Allgemeiner nennen wir jede reelle, nichtrationale Lösung der quadratischen Gleichung $ax^2 + bx + c = 0$ mit $a, b, c \in \mathbf{Z}$, $a \neq 0$, eine quadratische Irrationalität.

Der unendliche Kettenbruch $\alpha = [a_0; a_1, a_2, \ldots]$ heißt *periodisch*, wenn es ganze Zahlen $n \geqq 0$, $h \geqq 1$ gibt, so daß für beliebige $k \geqq n$ stets $a_{k+h} = a_k$ gilt. Wir schreiben dann

$$\alpha = [a_0; a_1, \ldots, a_{n-1}, \overline{a_n, \ldots, a_{n+h-1}}].$$

Satz 4.6. *Jeder periodische Kettenbruch stellt eine quadratische Irrationalität dar. Umgekehrt besitzt jede quadratische Irrationalität eine periodische Kettenbruchentwicklung.*

Beweis. 1. Es sei der periodische Kettenbruch

$$\alpha = [a_0; a_1, \ldots, a_{n-1}, \overline{a_n, \ldots, a_{n+h-1}}]$$

vorgelegt. Wir betrachten den aus den periodisch wiederkehrenden Elementen bestehenden Anteil des Kettenbruchs

$$\begin{aligned} r_n &= [a_n; a_{n+1}, \ldots, a_{n+h-1}, a_n, \ldots, a_{n+h-1}, \ldots] \\ &= [a_n; a_{n+1}, \ldots, a_{n+h-1}, r_n]. \end{aligned}$$

Für $h = 1$ ist

$$r_n = [a_n; r_n] = a_n + \frac{1}{r_n},$$

und r_n genügt der quadratischen Gleichung

$$r_n^2 - a_n r_n - 1 = 0.$$

Für $h > 1$ bezeichne $p''/q'', p'/q'$ die letzten beiden Näherungsbrüche von $[a_n; a_{n+1}, \ldots, a_{n+h-1}]$, wobei in diesem Kettenbruch ausnahmsweise $a_{n+h-1} = 1$ zugelassen ist. Nach Satz 4.1 ist dann

$$r_n = \frac{p' r_n + p''}{q' r_n + q''},$$

so daß auch in diesem Fall r_n einer quadratischen Gleichung

$$a r_n^2 + b r_n + c = 0$$

mit ganzzahligen Koeffizienten genügt. Aus

$$\alpha = [a_0; a_1, \ldots, a_{n-1}, r_n] = \frac{p_{n-1}r_n + p_{n-2}}{q_{n-1}r_n + q_{n-2}} \qquad (n \geqq 1)$$

bestimmt sich r_n zu

$$r_n = \frac{p_{n-2} - q_{n-2}\alpha}{q_{n-1}\alpha - p_{n-1}}.$$

Durch Einsetzen in die quadratische Gleichung für r_n erhält man eine solche für α mit ganzzahligen Koeffizienten:

$$A\alpha^2 + B\alpha + C = 0. \tag{8}$$

Da α durch einen unendlichen Kettenbruch gegeben war, ist α irrational. Also ist α eine quadratische Irrationalität.

2. Umgekehrt sei jetzt α als quadratische Irrationalität vorgegeben. α genügt also einer Gleichung (8) mit ganzzahligen Koeffizienten. Wir entwickeln α in einen Kettenbruch:

$$\alpha = [a_0; a_1, a_2, \ldots] = [a_0; a_1, \ldots, a_{n-1}, r_n] = \frac{p_{n-1}r_n + p_{n-2}}{q_{n-1}r_n + q_{n-2}}.$$

Durch Einsetzen in (8) erhält man eine quadratische Gleichung für r_n:

$$A_n r_n^2 + B_n r_n + C_n = 0. \tag{9}$$

Die ganzen Zahlen A_n, B_n, C_n errechnen sich zu

$$A_n = Ap_{n-1}^2 + Bp_{n-1}q_{n-1} + Cq_{n-1}^2,$$

$$B_n = 2Ap_{n-1}p_{n-2} + B(p_{n-1}q_{n-2} + p_{n-2}q_{n-1}) + 2Cq_{n-1}q_{n-2},$$

$$C_n = Ap_{n-2}^2 + Bp_{n-2}q_{n-2} + Cq_{n-2}^2 = A_{n-1}.$$

Dabei ist $A_n \neq 0$, denn sonst hätte (8) eine rationale Lösung. Wir zeigen jetzt, daß die Koeffizienten A_n, B_n, C_n beschränkt sind. Nach Satz 4.5 gibt es eine Zahl δ_{n-1} mit

$$p_{n-1} = \alpha q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}}$$

und $|\delta_{n-1}| < 1$. Damit ergibt sich für A_n

$$A_n = A\left(\alpha q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}}\right)^2 + B\left(\alpha q_{n-1} + \frac{\delta_{n-1}}{q_{n-1}}\right) q_{n-1} + Cq_{n-1}^2$$

$$= (A\alpha^2 + B\alpha + C)\, q_{n-1}^2 + 2A\alpha\delta_{n-1} + A\frac{\delta_{n-1}^2}{q_{n-1}^2} + B\delta_{n-1},$$

$$|A_n| < 2|A\alpha| + |A| + |B|.$$

Wegen $C_n = A_{n-1}$ ist noch

$$|C_n| < 2|A\alpha| + |A| + |B|.$$

Eine leichte Rechnung zeigt

$$B_n^2 - 4A_nC_n = (B^2 - 4AC)\,(p_{n-1}q_{n-2} - q_{n-1}p_{n-2})^2 = B^2 - 4AC.$$

Daher ist

$$B_n^2 \leqq 4\,|A_nC_n| + |B^2 - 4AC| < (2|A\alpha| + |A| + |B|)^2 + |B^2 - 4AC|.$$

Insgesamt können die Koeffizienten A_n, B_n, C_n nur endlich viele verschiedene Werte annehmen. Nach Gleichung (9) kommen dann aber auch für die r_n nur endlich viele verschiedene Werte in Frage. Ist für geeignete n und h etwa $r_n = r_{n+h}$ und

$$r_n = [a_n; a_{n+1}, \ldots],$$

$$r_{n+h} = [a_{n+h}; a_{n+h+1}, \ldots],$$

so folgt aus der Eindeutigkeit der Kettenbruchentwicklung $a_k = a_{k+h}$ für $k \geqq n$. Damit hat sich eine periodische Entwicklung ergeben.

4.2. Approximation reeller Zahlen durch rationale Zahlen

Prinzipiell läßt sich jede reelle Zahl mit beliebiger Genauigkeit durch rationale Zahlen approximieren, da die rationalen Zahlen in der Menge der reellen Zahlen dicht liegen. Das heißt, zu jeder reellen Zahl α und zu jedem $\varepsilon > 0$ finden sich rationale Zahlen p/q mit $|\alpha - p/q| < \varepsilon$. Es entsteht die Frage, was man bei Vorgabe von α und ε über die rationalen Zahlen p/q aussagen kann. Wir wollen die Frage nicht ausführlich diskutieren und erwähnen nur folgenden Satz.

Satz 4.7. *Zu beliebigen reellen Zahlen α und η mit $\eta \geqq 1$ gibt es ganze Zahlen p und q, die die Ungleichungen*

$$|q\alpha - p| < \frac{1}{\eta}, \qquad (1 \leqq q \leqq \eta)$$

erfüllen.

Beweis. Der Satz ist für rationale $\alpha = a/b$ mit $1 \leqq b \leqq \eta$ trivial. Wir können daher entweder α als rational mit $b > \eta$ oder als irrational annehmen. Wir betrachten die Näherungsbrüche p_k/q_k der Kettenbruchentwicklung von α und bestimmen zu η ein n aus $q_n \leqq \eta < q_{n+1}$. Nach (7) ist dann

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_nq_{n+1}} < \frac{1}{q_n\eta},$$

was der Behauptung des Satzes entspricht.

Eine andere Fragestellung ergibt sich, wenn man zu α eine Approximation p/q annimmt. Wie klein kann zu gegebenen α und q die Zahl ε in $|\alpha - p/q| < \varepsilon$ gemacht werden? Hierüber erhalten wir durch Satz 4.5 eine Auskunft: Approximiert man α durch Näherungsbrüche p_n/q_n seiner Kettenbruchentwicklung, so wird der Fehler

unter q_n^{-2} gedrückt. Wie sich zeigt, sind diese Approximationen in einem gewissen Sinne optimal.

Definition 4.2. Die rationale Zahl a/b, $(a, b) = 1$, $b > 0$, heißt *beste Approximation* der reellen Zahl α, wenn für alle rationalen Zahlen p/q mit $0 < q \leqq b$ und $p/q \neq a/b$ gilt

$$\left|\alpha - \frac{a}{b}\right| < \left|\alpha - \frac{p}{q}\right|.$$

Es besteht die bemerkenswerte Tatsache, daß die Näherungsbrüche der Kettenbruchentwicklung von α zugleich beste Approximationen dieser Zahl darstellen. Wir beweisen den in dieser Richtung bestehenden Satz von J. L. Lagrange (1736 bis 1813).

Satz 4.8 (Lagrange). *Ist p_n/q_n für $n \geqq 1$ ein Näherungsbruch von α, so gilt für alle rationalen Zahlen p/q mit $0 < q \leqq q_n$, $p/q \neq p_n/q_n$ die Ungleichung*

$$|q_n\alpha - p_n| < |q\alpha - p|.$$

Dieser Satz sagt etwas mehr aus als ursprünglich behauptet wurde. Aber aus

$$q_n\left|\alpha - \frac{p_n}{q_n}\right| < q\left|\alpha - \frac{p}{q}\right| \leqq q_n\left|\alpha - \frac{p}{q}\right|$$

folgt die Eigenschaft der besten Approximation von α durch p_n/q_n.

Beweis. Wir können sogleich $\alpha \neq p_n/q_n$ annehmen. Wir erfüllen die Gleichung

$$q\alpha - p = M(q_n\alpha - p_n) + N(q_{n-1}\alpha - p_{n-1}), \tag{10}$$

wenn M und N aus dem Gleichungssystem

$$Mp_n + Np_{n-1} = p$$
$$Mq_n + Nq_{n-1} = q$$

gewonnen werden. Da sich die Koeffizientendeterminante zu

$$\begin{vmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{vmatrix} = (-1)^{n-1}$$

ergibt, ist das System eindeutig lösbar, und überdies sind die Zahlen M und N ganz. Wegen $p/q \neq p_n/q_n$ muß $N \neq 0$ sein. Dann ist entweder $M = 0$ oder M und N haben verschiedene Vorzeichen, weil sonst entgegen der Voraussetzung $q > q_n$ wäre. Damit haben die Summanden auf der rechten Seite von (10) gleiche Vorzeichen. Denn auch die Klammerausdrücke haben verschiedene Vorzeichen, da es sich bei p_{n-1}/q_{n-1}, p_n/q_n um benachbarte Näherungsbrüche handelt. Daher ist

$$|q\alpha - p| = |M(q_n\alpha - p_n)| + |N(q_{n-1}\alpha - p_{n-1})| \geqq |q_{n-1}\alpha - p_{n-1}|.$$

In $\alpha = [a_0; a_1, \ldots, a_n, r_{n+1}]$ ist $r_{n+1} > 1$, da wir grundsätzlich nur solche Kettenbrüche betrachten. Aus

$$\alpha = \frac{p_n r_{n+1} + p_{n-1}}{q_n r_{n+1} + q_{n-1}}$$

folgt

$$r_{n+1} = -\frac{q_{n-1}\alpha - p_{n-1}}{q_n\alpha - p_n}$$

und

$$|q\alpha - p| \geqq |q_{n-1}\alpha - p_{n-1}| > |q_n\alpha - p_n|.$$

Dies beweist den Satz.

An Hand zweier Beispiele, der Zahlen $\sqrt{2}$ und π, soll die Nützlichkeit der besten Approximation demonstriert werden. Es werden jeweils die ersten drei Näherungsbrüche über die Formeln (1) und (2) als beste Approximationen angegeben und die Abschätzung des Fehlers nach Satz 4.5 vorgenommen.

1. Beste Approximationen von $\sqrt{2}$.

Wegen

$$\sqrt{2} = 1 + (\sqrt{2} - 1) = 1 + \frac{1}{2 + (\sqrt{2} - 1)}$$

besitzt $\sqrt{2}$ die periodische Kettenbruchentwicklung $\sqrt{2} = [1; 2]$. Daraus ergibt sich:

$$\frac{p_1}{q_1} = \frac{2 \cdot 1 + 1}{2 \cdot 1} = \frac{3}{2}, \qquad \left|\sqrt{2} - \frac{3}{2}\right| < \frac{1}{4} = 0{,}25;$$

$$\frac{p_2}{q_2} = \frac{2 \cdot 3 + 1}{2 \cdot 2 + 1} = \frac{7}{5}, \qquad \left|\sqrt{2} - \frac{7}{5}\right| < \frac{1}{25} = 0{,}04;$$

$$\frac{p_3}{q_3} = \frac{2 \cdot 7 + 3}{2 \cdot 5 + 2} = \frac{17}{12}, \qquad \left|\sqrt{2} - \frac{17}{12}\right| < \frac{1}{144} < 0{,}007.$$

2. Beste Approximationen von π.

Das allgemeine Bildungsgesetz des Kettenbruches von π ist nicht bekannt. Benutzt man eine genügende Anzahl von Stellen der Dezimalbruchentwicklung von π, so kann man die ersten Elemente des Kettenbruches ermitteln. Es ist $\pi = [3; 7, 15, 1, 292, \ldots]$. Daraus folgt

$$\frac{p_1}{q_1} = \frac{7 \cdot 3 + 1}{7 \cdot 1} = \frac{22}{7}, \qquad \left|\pi - \frac{22}{7}\right| < \frac{1}{49} < 0{,}021;$$

$$\frac{p_2}{q_2} = \frac{15 \cdot 22 + 3}{15 \cdot 7 + 1} = \frac{333}{106}, \qquad \left|\pi - \frac{333}{106}\right| < \frac{1}{106^2} < 0{,}00009;$$

$$\frac{p_3}{q_3} = \frac{1 \cdot 333 + 22}{1 \cdot 106 + 7} = \frac{355}{113}, \qquad \left|\pi - \frac{355}{113}\right| < \frac{1}{113^2} < 0{,}00008.$$

Bemerkenswert ist, daß die erste und dritte beste Approximation weit besser sind als die theoretischen Fehler angeben. So ist $\pi - 22/7 = -0{,}001\ldots$ und $\pi - 355/113 = -0{,}0000002\ldots$ Um so erstaunlicher ist, daß alle drei Approximationen als gute

Näherungen längst bekannt waren, bevor die Theorie der Kettenbrüche entwickelt war. Die Zahl 22/7 wurde von ARCHIMEDES (um 287—217 v. u. Z.) angegeben, und die Zahlen 333/106, 355/113 kannte bereits ADRIANUS METIUS (1571—1635).

Wir beziehen jetzt in die Betrachtung auch Approximationen p/q der reellen Zahl α mit

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^n}$$

ein, wobei n eine beliebige natürliche Zahl sein kann. Es wird die Frage nach der Beschaffenheit von α gestellt, wenn die Ungleichung bei vorgegebenem n unendlich viele Lösungen in rationalen Zahlen hat, wobei c von diesen nicht abhängen soll.

Definition 4.3. Die Zahl α ist *approximierbar durch rationale Zahlen zur Ordnung* n ($n \in \mathbf{N}$), wenn eine nur von α abhängende Konstante $c(\alpha)$ existiert, so daß

$$\left|\alpha - \frac{p}{q}\right| < \frac{c(\alpha)}{q^n}$$

unendlich viele Lösungen $p/q \in \mathbf{Q}$ besitzt.

Satz 4.9. *Eine rationale Zahl ist approximierbar zur Ordnung* 1 *und zu keiner höheren Ordnung.*

Beweis. Es sei $\alpha = a/b$ mit $(a, b) = 1$. Die lineare diophantische Gleichung $aq - bp = 1$ hat unendlich viele Lösungen p, q mit $(p, q) = 1$. Aus der Gleichung folgt

$$\frac{a}{b} - \frac{p}{q} = \frac{1}{bq}$$

und

$$\left|\frac{a}{b} - \frac{p}{q}\right| < \frac{2}{q},$$

so daß diese Ungleichung unendlich viele Lösungen besitzt. Also ist $\alpha = a/b$ approximierbar zur Ordnung 1. Sind $b, q > 0$ und $a/b \neq p/q$, so folgt

$$\left|\frac{a}{b} - \frac{p}{q}\right| = \frac{|aq - bp|}{bq} \geqq \frac{1}{bq}.$$

Eine Approximation zur Ordnung 2 erfordert $q < bc$. Diese Ungleichung läßt sich nur endlich oft realisieren. Daher kann eine rationale Zahl nicht zur Ordnung 2 approximierbar sein.

Satz 4.10. *Jede irrationale Zahl ist approximierbar zur Ordnung* 2.

Beweis. Jede irrationale Zahl besitzt eine unendliche Kettenbruchentwicklung. Nach Satz 4.5 liefern die Näherungsbrüche die gewünschten Approximationen.

Satz 4.11. *Eine quadratische Irrationalität ist nicht approximierbar zu einer Ordnung, die größer als 2 ist.*

Beweis. Die quadratische Irrationalität $\alpha = [a_0; a_1, a_2, \ldots]$ besitzt eine periodische Entwicklung, so daß ihre Teilnenner a_n beschränkt sind. Es sei $0 < a_n < M$ für alle $n \geqq 1$. Setzt man $\alpha = [a_0; a_1, \ldots, a_n, r_{n+1}]$, so ist nach dem Beweis zu Satz 4.4

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n(r_{n+1}q_n + q_{n-1})}.$$

Aus $r_{n+1} = a_{n+1} + \dfrac{1}{r_{n+2}} < a_{n+1} + 1$ folgt

$$\left|\alpha - \frac{p_n}{q_n}\right| > \frac{1}{q_n\big((a_{n+1}+1)\,q_n + q_{n-1}\big)} > \frac{1}{(M+2)\,q_n^2}.$$

Es sei nun p/q eine Approximation von α mit $q > 1$ und $q_{n-1} < q \leqq q_n$. Da p_n/q_n beste Approximation ist, so gilt

$$\left|\alpha - \frac{p}{q}\right| \geqq \left|\alpha - \frac{p_n}{q_n}\right| > \frac{1}{(M+2)\,q^2}\left(\frac{q}{q_n}\right)^2 > \frac{1}{(M+2)\,q^2}\left(\frac{q_{n-1}}{q_n}\right)^2$$
$$= \frac{1}{(M+2)\,q^2} \cdot \frac{1}{\left(a_n + \dfrac{q_{n-2}}{q_{n-1}}\right)^2} > \frac{1}{(M+2)^3\,q^2}.$$

Eine Approximation zur Ordnung 3 erfordert $q < (M+2)^3\,c$. Da sich diese Ungleichung aber nur endlich oft realisieren läßt, kann α nicht zur Ordnung 3 approximierbar sein.

4.3. Algebraische Zahlen

Definition 4.4. Eine Zahl α heißt *algebraische Zahl n-ten Grades*, wenn sie Wurzel einer Gleichung n-ten Grades

$$a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n = 0, \qquad a_0 \neq 0 \tag{11}$$

mit ganzzahligen Koeffizienten ist und keine Wurzel einer Gleichung niederen Grades.

Im Sinne dieser Definition sind die rationalen Zahlen algebraische Zahlen ersten Grades. Damit stellt der Begriff der algebraischen Zahl einer Verallgemeinerung des Begriffes der rationalen Zahl dar. Die quadratischen Irrationalitäten sind algebraische Zahlen zweiten Grades. Ist p eine Primzahl, so ist $\sqrt[n]{p}$ eine algebraische Zahl n-ten Grades. Auch $i = \sqrt{-1}$ als Lösung von $\alpha^2 + 1 = 0$ ist als algebraische Zahl anzusprechen. Jedoch interessieren wir uns hier nur für die reellen algebraischen Zahlen.

Satz 4.12. *Die Menge der algebraischen Zahlen ist abzählbar.*

Beweis. Wir definieren die *Höhe H* der Gleichung (11) durch

$$H := n + |a_0| + |a_1| + \cdots + |a_n|.$$

Das Minimum von H ist 2. Es gibt natürlich nur endlich viele Gleichungen einer festen Höhe H. Wir notieren sie uns durch $E_{H,1}, E_{H,2}, \ldots, E_{H,k_H}$. Nun können wir sämtliche Gleichungen in einer Folge anordnen: $E_{2,1}, E_{2,2}, \ldots, E_{2,k_2}$; $E_{3,1}, E_{3,2}, \ldots, E_{3,k_3}$; .... Damit ist die Menge der Gleichungen abzählbar. Da jede algebraische Zahl zu wenigstens einer Gleichung gehört und zu jeder Gleichung nur endlich viele algebraische Zahlen gehören, ist die Menge der algebraischen Zahlen ebenfalls abzählbar.

Im Jahre 1851 bewies J. Liouville (1809—1882) den folgenden, außerordentlich wichtigen Satz.

Satz 4.13 (Liouville). *Eine reelle algebraische Zahl n-ten Grades ist nicht approximierbar zu einer Ordnung, die größer als n ist.*

Beweis. Es genügt zu zeigen, daß es für beliebige ganzzahlige p und $q > 0$ eine Konstante K gibt mit

$$\left|\alpha - \frac{p}{q}\right| > \frac{K}{q^n},$$

wenn α eine reelle algebraische Zahl n-ten Grades ist. Es sei

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

und $f(\alpha) = 0$. Dann können wir $f(x) = (x - \alpha) f_1(x)$ mit $f_1(\alpha) \neq 0$ setzen. Es gibt eine Zahl δ mit $f_1(x) \neq 0$ in dem Intervall $\alpha - \delta \leqq x \leqq \alpha + \delta$. Dort sei $|f_1(x)| < M$. Es sei jetzt p/q $(q > 0)$ eine Approximation von α mit $\left|\alpha - \frac{p}{q}\right| \leqq \delta$. Dann ist

$$\left|\alpha - \frac{p}{q}\right| = \left|\frac{f\left(\frac{p}{q}\right)}{f_1\left(\frac{p}{q}\right)}\right| = \frac{|a_0p^n + a_1p^{n-1}q + \cdots + a_{n-1}pq^{n-1} + a_nq^n|}{\left|f_1\left(\frac{p}{q}\right)\right| q^n}$$

$$> \frac{1}{Mq^n} = \frac{K}{q^n}.$$

4.4. Transzendente Zahlen

Definition 4.5. Eine Zahl, die nicht algebraisch ist, heißt *transzendent*.

Der Satz von Liouville ist deswegen aus historischer Sicht von so grundlegender Bedeutung, da er zum ersten Mal die Existenz transzendenter Zahlen nachzuweisen erlaubte. Zu diesem Zweck konstruiere man eine Zahl, die sich in besonders guter Weise durch rationale Zahlen approximieren läßt. Ein Beispiel liefert nach [7] der folgende Satz.

Satz 4.14. *Die Zahl*

$$\alpha = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \cdots + \frac{1}{10^{n!}} + \cdots$$

ist transzendent.

Beweis. Wir setzen

$$\alpha_n = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \cdots + \frac{1}{10^{n!}} = \frac{p}{q}$$

mit $q = 10^{n!}$. Dann ist

$$0 < \alpha - \frac{p}{q} = \alpha - \alpha_n = \frac{1}{10^{(n+1)!}} + \frac{1}{10^{(n+2)!}} + \cdots < \frac{2}{10^{(n+1)!}} = \frac{2}{q^{n+1}}$$

und für alle $n > N$

$$0 < \alpha - \frac{p}{q} < \frac{2}{q^N}.$$

Da diese Ungleichung unendlich viele Lösungen hat, ist α approximierbar zur Ordnung N. Da man aber N beliebig groß wählen kann, ist α nicht algebraisch, also transzendent.

Etwa 20 Jahre nach LIOUVILLE zeigte G. CANTOR (1845—1918) wesentlich mehr, daß nämlich fast alle Zahlen transzendent sind. Gemeint ist damit, daß im Gegensatz zur Menge der algebraischen Zahlen die Menge der reellen Zahlen überabzählbar ist.

Satz 4.15 (CANTOR). *Die Menge der reellen Zahlen ist überabzählbar.*

Beweis. Es genügt, dies für die Zahlen x mit $0 \leqq x < 1$ zu zeigen. Jede derartige Zahl läßt sich als unendlicher Dezimalbruch schreiben. Dabei seien zwecks Forderung nach Eindeutigkeit unendlich viele aufeinanderfolgende Neunen ausgeschlossen. Ein endlicher Dezimalbruch werde durch Anhängen von Nullen zu einem unendlichen ergänzt. Wir nehmen entgegen der Behauptung an, die Menge der reellen Zahlen x mit $0 \leqq x < 1$ sei abzählbar. Wir können sie dann in einer gewissen Folge anordnen:

$$\begin{aligned} x_1 &= 0, a_{11}a_{12}a_{13} \ldots, \\ x_2 &= 0, a_{21}a_{22}a_{23} \ldots, \\ x_3 &= 0, a_{31}a_{32}a_{33} \ldots, \\ &\vdots \end{aligned}$$

Die a_{ik} stellen dabei die Ziffern der Dezimalbruchentwicklungen dar. Wir bilden jetzt den Dezimalbruch

$$x = 0, a_{11}a_{22}a_{33} \ldots$$

mit den auf der Diagonalen liegenden Ziffern. Nun ändern wir die Ziffern durch

$$b_n = \begin{cases} a_{nn} + 1 & \text{für } a_{nn} \neq 8,9 \\ 0 & \text{für } a_{nn} = 8,9 \end{cases}$$

ab. Die Zahl

$$y = 0, b_1 b_2 b_3 \ldots$$

ist von allen x_n verschieden, da jedenfalls die n-ten Ziffern verschieden sind. Das steht im Widerspruch zur Abzählbarkeit.

4.5. Die Irrationalität von e und π

Obwohl aus der im nächsten Abschnitt nachzuweisenden Transzendenz von e und π die Irrationalität folgt, sollen die Irrationalitätsbeweise doch gesondert geführt werden, da sie entschieden einfacher sind. Die Irrationalität von e und π wurde erstmals von J. H. Lambert (1728—1777) im Jahre 1761 bewiesen. Zum Beweis der Irrationalität von e benutzen wir eine einfache Variante von J. B. J. Fourier (1768—1830) und von π eine solche von J. Niven.

Satz 4.16 (Lambert). *Die Zahl e ist irrational.*

Beweis. Die Zahl e ist gegeben durch

$$e = \sum_{k=0}^{\infty} \frac{1}{k!}.$$

Wir nehmen an, e sei rational. Wir können $e = a/b$ mit $(a, b) = 1$ und $b > 1$ setzen, da $2 < e < 3$ ist. Mit $n \geqq b$ bilden wir die Zahl

$$\alpha = n! \left(e - \sum_{k=0}^{n} \frac{1}{k!} \right).$$

Diese Zahl ist sicher ganz. Andererseits steht

$$0 < \alpha = n! \sum_{k=n+1}^{\infty} \frac{1}{k!} < \sum_{k=n+1}^{\infty} \frac{1}{(n+1)^{k-n}} = \frac{1}{n} < 1$$

im Widerspruch zur Ganzzahligkeit von α.

Satz 4.17 (Lambert). *Die Zahl π ist irrational.*

Beweis. Wir nehmen an, π sei rational und setzen $\pi = a/b$, $(a, b) = 1$. Für beliebige natürliche Zahlen n werden die Polynome

$$f(x) = \frac{x^n (a - bx)^n}{n!},$$

$$F(x) = f(x) + \sum_{k=1}^{n} (-1)^k f^{(2k)}(x)$$

gebildet. Es ist

$$f(x) = \frac{1}{n!} \sum_{\nu=n}^{2n} c_\nu x^\nu$$

mit ganzen Zahlen c_ν. Folglich sind alle $f^{(k)}(0)$ für $k \geqq 0$ ganzzahlig. Da $f(\pi - x) = f\left(\frac{a}{b} - x\right) = f(x)$ ist, ist auch $f^{(k)}(\pi)$ ganzzahlig für $k \geqq 0$. Daher sind auch die beiden Werte $F(0)$, $F(\pi)$ ganzzahlig. Wegen

$$\frac{d}{dx}\left(F'(x) \sin x - F(x) \cos x\right) = \left(F''(x) + F(x)\right) \sin x = f(x) \sin x$$

ist

$$\int_0^\pi f(x) \sin x \, dx = F(\pi) + F(0) \in \mathbf{Z}.$$

Andererseits gilt für $0 < x < \pi$

$$0 < f(x) \sin x \leqq f(x) < \frac{\pi^n a^n}{n!}$$

und daher für hinreichend großes n

$$0 < \int_0^\pi f(x) \sin x \, dx < \frac{\pi^{n+1} a^n}{n!} < 1.$$

Dies steht im Widerspruch zur Ganzzahligkeit des Integrals.

4.6. Die Transzendenz von e und π

Die Transzendenz von e wurde im Jahre 1873 von C. HERMITE (1822—1901) und die Transzendenz von π im Jahre 1882 von F. LINDEMANN (1852—1939) bewiesen. Die Beweise wurden im Verlaufe der Jahre vereinfacht. Wir orientieren uns an der Darstellung in [15].

Hilfssatz 4.1. *Ist*

$$f(x) = \sum_{\nu=0}^{n} a_\nu x^\nu$$

ein beliebiges Polynom und

$$F(x) = \sum_{k=0}^{n} f^{(k)}(x),$$

dann gilt

$$|F(0) e^x - F(x)| \leqq e^{|x|} \sum_{\nu=0}^{n} |a_\nu| \, |x|^\nu.$$

Beweis. Aus

$$F(x) = \sum_{k=0}^{n} \sum_{\nu=k}^{n} a_\nu \frac{\nu!}{(\nu-k)!} x^{\nu-k} = \sum_{\nu=0}^{n} \nu! a_\nu \sum_{k=0}^{\nu} \frac{x^{\nu-k}}{(\nu-k)!}$$

$$= \sum_{\nu=0}^{n} \nu! a_\nu \sum_{k=0}^{\nu} \frac{x^k}{k!}$$

folgt

$$F(0) = \sum_{\nu=0}^{n} \nu! a_\nu$$

und damit

$$|F(0) e^x - F(x)| = \left| \sum_{\nu=0}^{n} \nu! a_\nu \sum_{k=0}^{\infty} \frac{x^k}{k!} - \sum_{\nu=0}^{n} \nu! a_\nu \sum_{k=0}^{\nu} \frac{x^k}{k!} \right|$$

$$= \left| \sum_{\nu=0}^{n} \nu! a_\nu \sum_{k=\nu+1}^{\infty} \frac{x^k}{k!} \right| \leqq \sum_{\nu=0}^{n} |a_\nu| \sum_{k=\nu+1}^{\infty} \frac{|x|^k}{(k-\nu)!}$$

$$< e^{|x|} \sum_{\nu=0}^{n} |a_\nu| \, |x|^\nu .$$

Satz 4.18 (Hermite). *Die Zahl e ist transzendent.*

Beweis. Es ist zu zeigen, daß für jedes Polynom

$$P(x) = \sum_{\mu=0}^{m} c_\mu x^\mu$$

mit $c_0 \neq 0$, $m > 0$ und ganzzahligen Koeffizienten $P(e) \neq 0$ ist. Es sei p eine Primzahl mit $p > \max(m, |c_0|)$. Wir bilden das Polynom

$$f(x) = \frac{x^{p-1}}{(p-1)!} \prod_{h=1}^{m} (h-x)^p = \sum_{\nu=0}^{n} a_\nu x^\nu$$

und entsprechend dem Hilfssatz

$$F(x) = \sum_{k=0}^{n} f^{(k)}(x).$$

Nun setzen wir

$$F(0) P(e) = A_1 + A_2 \tag{12}$$

mit

$$A_1 = \sum_{\mu=0}^{m} c_\mu F(\mu),$$

$$A_2 = \sum_{\mu=0}^{m} c_\mu \big(F(0) e^\mu - F(\mu)\big).$$

Es werden die beiden Summanden A_1, A_2 einzeln betrachtet. Beachtet man die Bildung des Polynoms $f(x)$ in

$$A_1 = \sum_{\mu=0}^{m} c_\mu \sum_{k=0}^{n} f^{(k)}(\mu),$$

so erkennt man, daß A_1 eine ganze Zahl sein muß. Aus

$$A_1 \equiv c_0(m!)^p \quad (p)$$

folgt wegen $c_0 \neq 0$, $p > \max(m, |c_0|)$, daß $A_1 \neq 0$ sein muß. Insgesamt ist $|A_1| \geqq 1$.

Bezüglich der Größe A_2 finden wir über den Hilfssatz

$$|F(0)\, e^\mu - F(\mu)| \leqq e^\mu \sum_{\nu=0}^{n} |a_\nu|\, \mu^\nu = e^\mu \frac{\mu^{p-1}}{(p-1)!} \prod_{h=1}^{m} (h+\mu)^p .$$

Die rechte Seite dieser Ungleichung geht für $p \to \infty$ gegen 0. Wählen wir also p hinreichend groß, so können wir stets $|A_2| < 1/2$ erreichen.

Aus (12) ergibt sich $P(e) \neq 0$ wegen $|A_1| \geqq 1$ und $|A_2| < 1/2$. Also kann e keiner algebraischen Gleichung genügen und muß transzendent sein.

Der Beweis der Transzendenz von π verläuft in entsprechenden Bahnen wie der vorstehende von e. Es wird insbesondere der zwischen e und π bestehende Zusammenhang $e^{\pi i} = -1$, $i = \sqrt{-1}$, ausgenutzt. Das bedeutet aber zugleich, daß der Transzendenzbeweis von π nicht mehr ganz von elementarem Charakter ist.

Satz 4.19 (Lindemann). *Die Zahl π ist transzendent.*

Beweis. Ist die reelle Zahl x algebraisch, so genügt sie einer Gleichung

$$\sum_{\mu=0}^{m} d_\mu x^\mu = 0$$

mit nicht sämtlich verschwindenden Koeffizienten $d_\mu \in \mathbf{Z}$. Für $y = ix$ ist

$$d_0 - id_1 y - d_2 y^2 + id_3 y^3 + d_4 y^4 - \cdots = 0$$

und daher

$$(d_0 - d_2 y^2 + d_4 y^4 - \cdots)^2 + (d_1 y - d_3 y^3 + d_5 y^5 - \cdots)^2 = 0 .$$

Also ist auch y algebraisch.

Nehmen wir jetzt an, daß π algebraisch ist, so ist auch πi algebraisch und Wurzel einer Gleichung

$$\sum_{\mu=0}^{m} c_\mu x^\mu = 0$$

mit $c_0, c_1, \ldots, c_m \in \mathbf{Z}$ und $c_m \neq 0$. Die Wurzeln dieser Gleichung werden mit $x_1, x_2, \ldots, x_m$ bezeichnet. Unter ihnen befindet sich neben der Wurzel πi auch die Wurzel $-\pi i$.

Wegen $e^{\pi i} = -1$ ist

$$\prod_{\mu=1}^{m} (1 + e^{x_\mu}) = 0.$$

Multiplizieren wir dieses Produkt aus, so erhalten wir

$$1 + \sum_{\nu=1}^{2^m-1} e^{y_\nu} = 0, \tag{13}$$

wobei die Zahlen y_ν die $2^m - 1$ Zahlen $x_1, x_2, \ldots, x_m, x_1 + x_2, x_1 + x_3, \ldots, x_1 + x_2 + \cdots + x_m$ in einer gewissen Reihenfolge durchlaufen. Wenigstens eine der Zahlen y_ν ist 0, denn wenigstens eine der Zahlen $x_\nu + x_\mu$ ist 0, da die Wurzeln πi und $-\pi i$ vorkommen. Wir können annehmen, daß $y_\nu \neq 0$ für $\nu = 1, 2, \ldots, n$ und $y_\nu = 0$ für $\nu = n + 1, n + 2, \ldots, 2^m - 1$. Wir setzen $q = 2^m - n$ und erhalten aus (13)

$$q + \sum_{\nu=1}^{n} e^{y_\nu} = 0. \tag{14}$$

In der Darstellung

$$g_n \prod_{\nu=1}^{n} (x - y_\nu) = \sum_{r=0}^{n} g_r x^r$$

sind die Koeffizienten g_r für $0 \leqq r \leqq n - 1$ abgesehen vom Vorzeichen die symmetrischen Grundfunktionen in $y_1, y_2, \ldots, y_n$. Sie sind also auch symmetrische Polynome in $y_1, y_2, \ldots, y_m$. Nach dem Hauptsatz über symmetrische Polynome (siehe [5]) sind sie ganze symmetrische Polynome in $x_1, x_2, \ldots, x_m$ und daher ganzzahlig. Natürlich ist $g_0 \neq 0$, $g_n \neq 0$.

Wir bringen jetzt wieder den Hilfssatz 4.1 in Anwendung und setzen mit einer Primzahl $p > \max(q, |g_0|, |g_n|)$

$$f(x) = \frac{g_n^{pn-1}}{(p-1)!} x^{p-1}(g_0 + g_1 x + \cdots + g_n x^n)^p.$$

Entsprechend dem Hilfssatz werde $F(x)$ durch die Summe der Ableitungen von $f(x)$ gebildet. Wir betrachten jetzt die Zahl

$$A = qF(0) + \sum_{\nu=1}^{n} F(y_\nu). \tag{15}$$

Nach Hilfssatz 4.1 und (14) ist

$$|A| = \left| \sum_{\nu=1}^{n} \left(F(y_\nu) - e^{y_\nu} F(0) \right) \right| \leqq \sum_{\nu=1}^{n} e^{|y_\nu|} h(y_\nu)$$

mit

$$h(x) = \frac{|g_n|^{pn-1}}{(p-1)!} |x|^{p-1}(|g_0| + |g_1|\,|x| + \cdots + |g_n|\,|x|^n)^p.$$

Ist $y = \max(|y_1|, |y_2|, \ldots, |y_n|)$, so ergibt sich

$$|A| \leqq n e^y h(y).$$

Da $h(y)$ für große p beliebig klein wird, kann man $|A| < 1$ für hinreichend großes p erreichen. Daraus erzielen wir einen Widerspruch, wenn wir zeigen können, daß A eine ganze, nicht durch p teilbare Zahl ist.

Die Zahl $qF(0)$ in der Darstellung (15) von A ist ganz und wegen

$$qF(0) \equiv qg_n{}^{pn-1}g_0{}^p \quad (p)$$

und $p > \max(q, |g_0|, |g_n|)$ nicht durch p teilbar.

Es verbleibt noch zu zeigen, daß die Zahl $\sum_{\nu=1}^{n} F(y_\nu)$ in (15) ganz und durch p teilbar ist. Dann ist A ganz und nicht durch p teilbar, was im Widerspruch zu $|A| < 1$ steht. Wegen

$$g_0 + g_1 x + \cdots + g_n x^n = g_n(x - y_1)(x - y_2) \cdot \cdots \cdot (x - y_n)$$

ist

$$f(x) = \frac{(g_n x)^{p-1}}{(p-1)!}(g_n x - g_n y_1)^p (g_n x - g_n y_2)^p \cdot \cdots \cdot (g_n x - g_n y_n)^p.$$

Diesen Ausdruck entwickeln wir nach Potenzen von $g_n x - g_n y_\nu$ $(1 \leqq \nu \leqq n)$ und erhalten

$$f(x) = \sum_{\mu=p}^{np+p-1} \frac{a_{\nu\mu}}{\mu!}(g_n x - g_n y_\nu)^\mu.$$

Die Koeffizienten $a_{\nu\mu}$ sind selbst Polynome in $g_n y_1, g_n y_2, \ldots, g_n y_n$ mit ganzzahligen, durch p teilbaren Koeffizienten. Darüber hinaus stellen sie symmetrische Funktionen (vgl. [5]) der Größen $y_1, \ldots, y_{\nu-1}, y_{\nu+1}, \ldots, y_n$ dar. Es ist

$$F(y_\nu) = \sum_{\mu=p}^{np+p-1} a_{\nu\mu} g_n{}^\mu$$

und

$$\sum_{\nu=1}^{n} F(y_\nu) = \sum_{\mu=p}^{np+p-1} g_n{}^\mu \sum_{\nu=1}^{n} a_{\nu\mu}. \tag{16}$$

Die innere Summe bildet eine ganze symmetrische Funktion von $g_n y_1, g_n y_2, \ldots, g_n y_n$ mit ganzzahligen, durch p teilbaren Koeffizienten. Sie und damit (16) ist selbst eine ganze, durch p teilbare Zahl. Denn zu den Wurzeln $g_n y_1, g_n y_2, \ldots, g_n y_n$ gehört die Gleichung

$$g_0 g_n{}^{n-1} + g_1 g_n{}^{n-2} x + \cdots + g_{n-2} g_n x^{n-2} + g_{n-1} x^{n-1} + x^n = 0,$$

deren höchster Koeffizient 1 ist.

Da die ganze Zahl A nicht durch p teilbar ist, muß sie von 0 verschieden sein. Dann kann aber nicht $|A| < 1$ sein.

4.7. Aufgaben

1. Man zeige: Ist die natürliche Zahl N keine Quadratzahl, so ist $\sqrt{N}$ irrational.
2. Man zeige: Sind n, m verschiedene natürliche Zahlen mit $(n, m) > 1$, so ist $\log_n m$ irrational.
3. Die reelle Zahl x sei Wurzel einer Gleichung

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$$

mit ganzzahligen Koeffizienten. Es ist zu zeigen, daß x entweder ganz oder irrational ist.

4. Man bestimme die ersten drei besten Approximationen von $\sqrt{3}$, $\sqrt{5}$, $\sqrt{7}$.
5. Man berechne $[2; \overline{1, 1, 3}]$, $[6; \overline{3, 12}]$, $[4; \overline{2, 8}]$.
6. Man beweise für natürliche Zahlen n:

$$\sqrt{n^2 + 1} = [n; \overline{2n}], \sqrt{n^2 + 2} = [n; \overline{n, 2n}].$$

5. Zahlentheoretische Funktionen

In den vorangegangenen Kapiteln ist uns bereits eine Reihe von zahlentheoretischen Funktionen, das heißt Funktionen, die für alle natürlichen Werte ihres Argumentes erklärt sind, begegnet. Es handelte sich um die Eulersche φ-Funktion $\varphi(n)$, die Anzahl der nichtisomorphen abelschen Gruppen n-ter Ordnung $a(n)$, die Anzahl $\Omega(n)$ der Primfaktoren von n beziehungsweise die Anzahl $\omega(n)$ der verschiedenen Primfaktoren und die Restklassencharaktere $\chi(n)$. In diesem Kapitel werden wir weitere für die Zahlentheorie wichtige Funktionen kennenlernen. In den ersten beiden Abschnitten betrachten wir vorwiegend allgemeinere Aussagen. Im großen vierten Abschnitt führen wir zunächst ganz einfache Abschätzungen der Anzahl der Primzahlen unterhalb einer Schranke durch, vertiefen diese durch die Ergebnisse von ČEBYŠEV und gelangen schließlich zum elementaren, aber schwierigen Beweis des Primzahlsatzes. Der vorangestellte dritte Abschnitt stellt einige Hilfsmittel zur Abschätzung von Summen bereit. Die folgenden Abschnitte befassen sich mit der Beurteilung zahlentheoretischer Funktionen für große Werte ihrer Argumente. Im allgemeinen ergeben sich dabei keine klaren Resultate, da die Funktionswerte selbst benachbarter Argumente erheblich differieren können. Aus diesem Grunde hat man gewisse Größenordnungsbegriffe geschaffen, die doch in bestimmten Maßen Auskunft über die Größenverhältnisse der Funktionswerte geben. Es sind dies die maximale, durchschnittliche und normale Größenordnung, die an einzelnen wichtigen zahlentheoretischen Funktionen demonstriert werden sollen.

5.1. Dirichletsche Multiplikation zahlentheoretischer Funktionen

Definition 5.1. Eine *zahlentheoretische Funktion* ist eine auf der Menge der natürlichen Zahlen erklärte, reell- oder komplexwertige Funktion.

Wir betrachten jetzt eine nach P. G. L. DIRICHLET (1805—1859) benannte zweckmäßige Verknüpfungsvorschrift zahlentheoretischer Funktionen.

Definition 5.2. Sind $f(n)$ und $g(n)$ zwei zahlentheoretische Funktionen, so bezeichne die zahlentheoretische Funktion

$$h(n) := \sum_{t|n} f(t)\, g\left(\frac{n}{t}\right)$$

ihr *Dirichletsches Produkt*. Dabei ist die Summe über alle Teiler t von n zu erstrecken. Für $h(n)$ wird auch $h(n) = f(n) * g(n)$ oder kürzer $h = f * g$ geschrieben.

Durchläuft t die Teiler von n, so $\frac{n}{t}$ die Komplementärteiler. Wir können so auch

$$f(n) * g(n) = \sum_{td=n} f(t)\, g(d)$$

schreiben, wobei die Summe über alle natürlichen Zahlen t, d gebildet wird, die der Gleichung $td = n$ genügen. Aus dieser Darstellung erkennt man sofort, daß die Dirichletsche Multiplikation *kommutativ* ist. Sie ist auch *assoziativ*, was aus

$$f(n) * \big(g(n) * h(n)\big) = f(n) * \sum_{t_1 t_2 = n} g(t_1)\, h(t_2) = \sum_{t_3 d = n} f(t_3) \sum_{t_1 t_2 = d} g(t_1)\, h(t_2)$$

$$= \sum_{t_1 t_2 t_3 = n} g(t_1)\, h(t_2)\, f(t_3)$$

folgt. Die Funktion

$$\varepsilon(n) = \begin{cases} 1 & \text{für } n = 1, \\ 0 & \text{für } n > 1 \end{cases}$$

übernimmt die Rolle des *Einselementes*, denn es ist

$$\varepsilon(n) * f(n) = \sum_{t \mid n} \varepsilon(t)\, f\left(\frac{n}{t}\right) = f(n).$$

In der Menge der zahlentheoretischen Funktionen $f(n)$ mit $f(1) \neq 0$ ist das Einselement eindeutig bestimmt. Denn gäbe es neben $\varepsilon(n)$ noch eine Funktion $\varepsilon_1(n)$ mit $\varepsilon_1(n) * f(n) = f(n)$, so wäre

$$\big(\varepsilon(n) - \varepsilon_1(n)\big) * f(n) = \sum_{t \mid n} \big(\varepsilon(t) - \varepsilon_1(t)\big)\, f\left(\frac{n}{t}\right) = 0.$$

Für $n = 1$ liest man hieraus wegen $f(1) \neq 0$ sofort $\varepsilon_1(1) = \varepsilon(1)$ ab. Sei bereits $\varepsilon_1(h) = \varepsilon(h)$ für $h < n$ festgestellt, so folgt $\varepsilon_1(n) = \varepsilon(n)$ wiederum wegen $f(1) \neq 0$. Also ist $\varepsilon_1(n) = \varepsilon(n)$ für alle n. Für $f(1) \neq 0$ läßt sich die Gleichung $f(n) * x(n) = \varepsilon(n)$ eindeutig nach $x(n)$ auflösen. Denn aus

$$\sum_{t \mid n} f\left(\frac{n}{t}\right) x(t) = \begin{cases} 1 & \text{für } n = 1, \\ 0 & \text{für } n > 1 \end{cases}$$

folgt $x(1) = \dfrac{1}{f(1)}$, und für $n > 1$ ist $x(n)$ aus

$$x(n) = -\frac{1}{f(1)} \sum_{\substack{t \mid n \\ t < n}} f\left(\frac{n}{t}\right) x(t)$$

durch Rekursion eindeutig bestimmt. Wir bezeichnen $x(n)$ als die zu $f(n)$ *inverse Funktion* und schreiben $x(n) = f^{-1}(n)$. Insgesamt hat sich ergeben:

Satz 5.1. *Die Menge der zahlentheoretischen Funktionen $f(n)$ mit $f(1) \neq 0$ bildet bezüglich der Dirichletschen Multiplikation eine abelsche Gruppe.*

Definition 5.3. Eine nicht identisch verschwindende zahlentheoretische Funktion $f(n)$ heißt *multiplikativ*, wenn $f(n_1 n_2) = f(n_1) f(n_2)$ für $(n_1, n_2) = 1$ gilt. Die Funktion heißt *total multiplikativ*, wenn $f(n_1 n_2) = f(n_1) f(n_2)$ ohne jede Einschränkung besteht.

Für eine multiplikative Funktion $f(n)$ ist stets $f(1) = 1$. Denn es gibt ein m mit $f(m) \neq 0$. Für dieses m ist $f(1 \cdot m) = f(1) f(m)$, also $f(1) = 1$.

Satz 5.2. *Sind $f(n)$ und $g(n)$ multiplikativ, so auch $f(n) * g(n)$.*

Beweis. Es sei $n = n_1 n_2$ mit $(n_1, n_2) = 1$. In

$$h(n_1 n_2) = \sum_{t \mid n_1 n_2} f(t)\, g\left(\frac{n_1 n_2}{t}\right)$$

kann t in $t = t_1 t_2$ mit $(t_1, t_2) = 1$ so zerlegt werden, daß t_1 die Teiler von n_1 und t_2 die Teiler von n_2 durchlaufen. Dann ist

$$h(n_1 n_2) = \sum_{t_1 \mid n_1} \sum_{t_2 \mid n_2} f(t_1)\, f(t_2)\, g\left(\frac{n_1}{t_1}\right) g\left(\frac{n_2}{t_2}\right) = h(n_1)\, h(n_2).$$

Es ist zu beachten, daß sich die totale Multiplikativität von zwei Funktionen im allgemeinen nicht auf ihr Dirichletsches Produkt überträgt. Zum Beispiel ist die Funktion $f(n) = n$ total multiplikativ, aber nicht $h(n) = n * n$. Dies erkennt man etwa aus $h(2) = 4$, $h(4) = 12$, $h(4) \neq h(2)\, h(2)$.

Definition 5.4. Für beliebige reelle k werden die *Teilerfunktionen* durch

$$\sigma_k(n) := 1 * n^k = \sum_{t \mid n} t^k$$

erklärt.

Insbesondere beschreibt $\sigma_0(n)$ die Anzahl der Teiler von n. Üblicherweise wird $\sigma_0(n) = d(n)$ geschrieben. Für die Summe der Teiler von n $\sigma_1(n)$ wird auch nur $\sigma(n)$ verwendet.

Da die Funktionen 1 und n^k multiplikativ sind, ist auch $\sigma_k(n)$ multiplikativ. Für eine Primzahlpotenz $n = p^\nu$ ist

$$\sigma_k(p^\nu) = 1 + p^k + p^{2k} + \cdots + p^{\nu k} = \begin{cases} \dfrac{p^{k(\nu+1)} - 1}{p^k - 1} & \text{für } k \neq 0 \\ \nu + 1 & \text{für } k = 0. \end{cases}$$

Kennt man also die kanonische Zerlegung von n,

$$n = \prod_{i=1}^{r} p_i^{\nu_i},$$

so ist für $k \neq 0$

$$\sigma_k(n) = \prod_{i=1}^{r} \frac{p_i^{k(\nu_i+1)} - 1}{p_i^k - 1}$$

und für $k = 0$

$$d(n) = \prod_{i=1}^{r} (\nu_i + 1).$$

Satz 5.3. *Sind $g(n)$ und $f(n) * g(n)$ multiplikativ, so auch $f(n)$.*

Beweis. Im Hinblick auf Satz 5.2 zeigen wir, daß $h(n) = f(n) * g(n)$ nicht multiplikativ ist, wenn $f(n)$ nicht multiplikativ ist. Es seien die Zahlen n_1, n_2 mit $(n_1, n_2) = 1$ so ausgewählt, daß $f(n_1 n_2) \neq f(n_1) f(n_2)$ ist und das Produkt $n_1 n_2$ minimal ausfällt. Ist $n_1 n_2 = 1$, so ist $h(1) = f(1) g(1) = f(1) \neq 1$, also $h(n)$ nicht multiplikativ. Ist $n_1 n_2 > 1$, so ist $f(n_1' n_2') = f(n_1') f(n_2')$ für $(n_1', n_2') = 1$ und $n_1' n_2' < n_1 n_2$. Daraus folgt

$$\begin{aligned} h(n_1 n_2) &= \sum_{\substack{t_1 \mid n_1 \, t_2 \mid n_2 \\ t_1 t_2 < n_1 n_2}} \sum f(t_1 t_2)\, g\left(\frac{n_1 n_2}{t_1 t_2}\right) + f(n_1 n_2) \\ &= \sum_{t_1 \mid n_1} \sum_{t_2 \mid n_2} f(t_1)\, f(t_2)\, g\left(\frac{n_1}{t_1}\right) g\left(\frac{n_2}{t_2}\right) - f(n_1)\, f(n_2) + f(n_1 n_2) \\ &= h(n_1)\, h(n_2) - f(n_1)\, f(n_2) + f(n_1 n_2) \neq h(n_1)\, h(n_2). \end{aligned}$$

Wir definieren jetzt eine für die Primzahltheorie bedeutsame Funktion, die nach A. F. Möbius (1790–1868) benannt wurde.

Definition 5.5. Die zu $f(n) \equiv 1$ inverse Funktion werde als *Möbiussche μ-Funktion* bezeichnet.

Für die μ-Funktion besteht also die Beziehung $1 * \mu(n) = \varepsilon(n)$ oder ausführlicher

$$\sum_{t \mid n} \mu(t) = \begin{cases} 1 & \text{für } n = 1, \\ 0 & \text{für } n > 1. \end{cases}$$

Da $f(n) \equiv 1$ und $\varepsilon(n)$ multiplikativ sind, ist nach Satz 5.3 auch $\mu(n)$ multiplikativ. Berechnen wir $\mu(n)$ für Primzahlpotenzen $n = p^r$. Aus der definierenden Gleichung ergibt sich

$$\mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^r) = 0.$$

Wegen $\mu(1) = 1$ erhält man hieraus für $r = 1$ $\mu(p) = -1$ und sukzessive $\mu(p^k) = 0$ für $k > 1$. Benutzen wir die kanonische Zerlegung

$$n = \prod_{i=1}^{r} p_i^{\nu_i},$$

so erhalten wir für $n > 1$

$$\mu(n) = \begin{cases} (-1)^r & \text{für } \nu_1 = \nu_2 = \cdots = \nu_r = 1, \\ 0 & \text{sonst.} \end{cases}$$

Mit Hilfe der Möbiusschen μ-Funktion läßt sich die inverse Funktion einer total multiplikativen Funktion leicht bestimmen.

Satz 5.4. *Ist $g(n)$ total multiplikativ, so ist $g^{-1}(n) = \mu(n)\, g(n)$.*

Beweis.

$$\big(\mu(n)\, g(n)\big) * g(n) = \sum_{t \mid n} \mu(t)\, g(t)\, g\left(\frac{n}{t}\right) = g(n) \sum_{t \mid n} \mu(t) = \varepsilon(n).$$

Hieraus ergibt sich sofort:

Satz 5.5 (Möbiussche Formeln). Ist $g(n)$ *total multiplikativ, so gilt:*

$$F(n) = f(n) * g(n) \Leftrightarrow f(n) = F(n) * \big(\mu(n)\, g(n)\big).$$

Betrachten wir die Gleichung $F(n) = f(n) * g(n)$ und ihre Auflösung nach $f(n)$ gemäß Satz 5.5 unter der zusätzlichen Voraussetzung, daß entweder $f(n)$ oder $F(n)$ multiplikativ ist. Nach den Sätzen 5.2 und 5.3 ist dann jeweils die andere Funktion auch multiplikativ. Es genügt also, $f(n)$ aus $f(n) = F(n) * \big(\mu(n)\, g(n)\big)$ für Primzahlpotenzen zu berechnen. Für $n = p^r$ ist

$$f(p^r) = \sum_{t \mid p^r} \mu(t)\, g(t)\, F\left(\frac{p^r}{t}\right) = F(p^r) - g(p)\, F(p^{r-1}).$$

Mit der kanonischen Zerlegung

$$n = \prod_{i=1}^{r} p_i^{\nu_i}$$

ergibt sich

$$f(n) = \prod_{i=1}^{r} \big(F(p_i^{\nu_i}) - g(p_i)\, F(p_i^{\nu_i - 1})\big).$$

Die Eulersche φ-Funktion:

In Abschnitt 2.2 haben wir die Eulersche φ-Funktion kennengelernt. Setzen wir lediglich die Kenntnis von Satz 2.5, also $1 * \varphi(n) = n$, voraus, so beherrschen wir unter den neuen Gesichtspunkten $\varphi(n)$ völlig. Da 1 und n multiplikative Funktionen sind, ist nach Satz 5.3 auch $\varphi(n)$ multiplikativ. Die Anwendung der Möbiusschen Formeln gibt $\varphi(n) = n * \mu(n)$ und

$$\varphi(n) = \prod_{i=1}^{r} (p_i^{\nu_i} - p_i^{\nu_i - 1}) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

Definition 5.6. Die durch $1 * \Lambda(n) = \log n$ eindeutig bestimmte Funktion $\Lambda(n)$ werde als *Mangoldtsche Funktion* bezeichnet.

Wie wir später sehen werden, spielt diese Funktion in der Primzahltheorie eine bedeutende Rolle. Wegen $\Lambda(1) = 0$ ist die Mangoldtsche Funktion nicht multiplikativ. Aus den Möbiusschen Formeln finden wir

$$\Lambda(n) = \mu(n) * \log n = \sum_{t \mid n} \mu(t) \log \frac{n}{t} = -\sum_{t \mid n} \mu(t) \log t. \tag{1}$$

Hieraus können wir $\Lambda(n)$ berechnen. Zunächst sei n eine Primzahlpotenz $n = p^r$. Man erkennt sofort

$$\Lambda(p^r) = \log p.$$

Ist n eine zusammengesetzte Zahl, so kann man n durch $n = n_1 n_2$ mit $1 < n_1 < n$ und $(n_1, n_2) = 1$ darstellen. In (1) zerlegen wir ebenso die Teiler t durch $t = t_1 t_2$, indem t_1 die Teiler von n_1 und t_2 die Teiler von n_2 durchlaufen. So ist

$$\Lambda(n_1 n_2) = -\sum_{t_1 | n_1} \sum_{t_2 | n_2} \mu(t_1)\,\mu(t_2)\,(\log t_1 + \log t_2) = 0$$

wegen $1 * \mu(n) = 0$ für $n > 1$.

5.2. Dirichletsche Reihen

Definition 5.7. Es sei $f(n)$ eine zahlentheoretische Funktion. Die unendliche Reihe $\sum_{n=1}^{\infty} \frac{f(n)}{n^s}$ heiße die $f(n)$ zugeordnete *Dirichletsche Reihe*.

Als bekannt sei vorausgesetzt, daß aus der absoluten Konvergenz einer Dirichletschen Reihe für $s = s_0$ die absolute Konvergenz für $s > s_0$ folgt. Damit entspricht jeder zahlentheoretischen Funktion $f(n)$, die eine irgendwo konvergente, zugeordnete Dirichletsche Reihe besitzt, eindeutig eine Funktion

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

der reellen Variablen s. Daß auch umgekehrt jeder durch eine Dirichletsche Reihe darstellbaren Funktion eindeutig eine zahlentheoretische Funktion entspricht, zeigt folgender Satz.

Satz 5.6. *Ist*

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} = 0$$

für alle $s > s_0$, *so ist* $f(n) = 0$.

Beweis. Im Gegensatz zur Behauptung nehmen wir $f(n) = 0$ für $n < m$, aber $f(m) \neq 0$ an. Dann ist für $s > s_0$

$$0 = \frac{f(m)}{m^s} + \sum_{n=m+1}^{\infty} \frac{f(n)}{n^s} = \frac{f(m)}{m^s} + \sum_{k=1}^{\infty} \frac{f(m+k)}{(m+k)^s} = \frac{f(m)}{m^s}\left(1 + G(s)\right) \tag{2}$$

mit

$$G(s) = \sum_{k=1}^{\infty} \frac{f(m+k)}{f(m)} \left(\frac{m}{m+k}\right)^s.$$

Genügt s_1 der Ungleichung $s_0 < s_1 < s$, so ist

$$\left(\frac{m}{m+k}\right)^{s} = \left(\frac{m}{m+k}\right)^{s-s_1}\left(\frac{m}{m+k}\right)^{s_1} \leqq \left(\frac{m}{m+1}\right)^{s-s_1}\left(\frac{m}{m+k}\right)^{s_1}$$

und daher

$$|G(s)| \leqq \left(\frac{m}{m+1}\right)^{s-s_1} \frac{m^{s_1}}{|f(m)|} \sum_{k=1}^{\infty} \frac{|f(m+k)|}{(m+k)^{s_1}}.$$

Hieraus erkennt man, daß $G(s)$ mit $s \to \infty$ gegen 0 strebt. Daher kann man in (2) $|1 + G(s)| > 1/2$ für genügend großes s sichern. Dann steht aber Gleichung (2) im Widerspruch zur Annahme $f(m) \neq 0$, und der Satz ist bewiesen.

Der aufgeführte Zusammenhang zwischen zahlentheoretischer Funktion und Funktion einer reellen Veränderlichen eröffnet weitreichende Möglichkeiten zur Untersuchung zahlentheoretischer Funktionen. Wir zeigen zunächst, daß die im vorangegangenen Abschnitt eingeführte Dirichletsche Multiplikation, die im ersten Moment etwas merkwürdig erscheinen muß, über die Dirichletschen Reihen ihre ganz natürliche Erklärung findet. Seien die die Funktionen $F(s)$ und $G(s)$ darstellenden Dirichletschen Reihen

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

für $s > s_0$ absolut konvergent. Bekanntlich konvergiert dann auch jede Reihe, die die Produkte $\frac{f(n)}{n^s} \cdot \frac{g(m)}{m^s}$ in beliebiger Reihenfolge durchläuft, für $s > s_0$ absolut, und zwar gegen das Produkt $F(s)\,G(s)$. Damit kann man das Produkt $F(s)\,G(s)$ in der Form

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

bilden. Schreibt man

$$F(s)\,G(s) = H(s) = \sum_{k=1}^{\infty} \frac{h(k)}{k^s},$$

so ist $h(n) = f(n) * g(n)$. Also entsprechen sich Dirichletsche Multiplikation und Multiplikation Dirichletscher Reihen. Natürlich ist die von den Dirichletschen Reihen unabhängige Definition der Dirichletschen Multiplikation allgemeiner, da sie an keine Konvergenzbedingungen gebunden ist. Im Falle der Konvergenz kann aber aus der Gleichheit $H(s) = F(s)\,G(s)$ auf die Gleichheit $h(n) = f(n) * g(n)$ und umgekehrt geschlossen werden. Auch die Auflösung der zahlentheoretischen Gleichung nach $f(n)$ kann über die Auflösung $F(s) = \dfrac{H(s)}{G(s)}$ im allgemeinen einfach durch Darstellung von $\dfrac{1}{G(s)}$ in Form einer Dirichletschen Reihe vorgenommen werden.

Bevor auf Beispiele eingegangen wird, soll noch eine wichtige Produktdarstellung im Fall multiplikativer zahlentheoretischer Funktionen aufgestellt werden.

Es sei $f(n)$ multiplikativ und $\sum_{n=1}^{\infty} f(n)\, n^{-s}$ für $s > s_0$ absolut konvergent. Wir bilden mit einer Primzahl p

$$F_p(s) := \sum_{\nu=0}^{\infty} \frac{f(p^\nu)}{p^{\nu s}}$$

für $s > s_0$ und das Produkt von $F_p(s)$ über alle Primzahlen, welche die r-te Primzahl p_r nicht überschreiten:

$$\prod_{p \leqq p_r} F_p(s) = \sum_{\nu_1=0}^{\infty} \cdots \sum_{\nu_r=0}^{\infty} \frac{f(p_1^{\nu_1}) \cdot \ldots \cdot f(p_r^{\nu_r})}{p_1^{\nu_1 s} \cdot \ldots \cdot p_r^{\nu_r s}}.$$

Auf Grund der Multiplikativität von $f(n)$ können wir auch

$$\prod_{p \leqq p_r} F_p(s) = \sum_{r} \frac{f(n)}{n^s}$$

schreiben, wobei die Summe über alle diejenigen natürlichen Zahlen zu erstrecken ist, die durch Primzahlen $p \leqq p_r$ gebildet werden. Da die rechte Seite der Ungleichung

$$\left| \sum_{n=1}^{\infty} \frac{f(n)}{n^s} - \sum_{r} \frac{f(n)}{n^s} \right| \leqq \sum_{n=p_r+1}^{\infty} \frac{|f(n)|}{n^s}$$

für $r \to \infty$ gegen 0 strebt, geht $\sum_r f(n)\, n^{-s}$ für $r \to \infty$ gegen $\sum_{n=1}^{\infty} f(n)\, n^{-s}$. Das Produkt konvergiert, sofern die Summe der Logarithmen konvergent ist. Mit $\log(1+x) \leqq x$ für $x > -1$ ergibt sich

$$\left| \log \prod_{p \leqq p_r} F_p(s) \right| \leqq \sum_{p \leqq p_r} |\log F_p(s)| = \sum_{p \leqq p_r} \left| \log \left(1 + \sum_{\nu=1}^{\infty} \frac{f(p^\nu)}{p^{\nu s}} \right) \right|$$

$$\leqq \sum_{p \leqq p_r} \sum_{\nu=1}^{\infty} \frac{|f(p^\nu)|}{p^{\nu s}} \leqq \sum_{n=2}^{\infty} \frac{|f(n)|}{n^s}.$$

Aus der Beschränktheit der Partialsummen folgt die Konvergenz von Reihe und Produkt. Damit ist

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p} F_p(s),$$

wobei das Produkt über alle Primzahlen zu erstrecken ist. Für total multiplikative Funktionen ist noch

$$F_p(s) = \frac{1}{1 - f(p)\, p^{-s}}.$$

Insgesamt fassen wir zusammen:

Satz 5.7. *Ist $f(n)$ eine multiplikative zahlentheoretische Funktion, und ist $\sum_{n=1}^{\infty} f(n)\, n^{-s}$ für $s > s_0$ absolut konvergent, dann gilt für $s > s_0$*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \left(\sum_{\nu=0}^{\infty} \frac{f(p^\nu)}{p^{\nu s}} \right).$$

Ist überdies $f(n)$ total multiplikativ, so ist

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_p \frac{1}{1 - f(p)\, p^{-s}}.$$

Definition 5.8. Als *Riemannsche Zetafunktion* werde die für $s > 1$ erklärte Funktion

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

bezeichnet.

Diese von B. RIEMANN (1826—1866) ausgiebig untersuchte Funktion spielt in der Primzahltheorie eine grundlegende Rolle, was aber in diesem Buch nicht dargelegt werden soll. Wir werden sie zur Erzeugung von zahlentheoretischen Funktionen ausnutzen. Die aus Satz 5.7 folgende *Produktdarstellung*

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}$$

war schon L. EULER bekannt.

Die Möbiussche μ-Funktion:

Aus $1 * \mu(n) = \varepsilon(n)$ folgt für $s > 1$

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

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

Die Teilerfunktionen:

Für $s > \max(1, k+1)$ ist

$$\zeta(s)\, \zeta(s-k) = \sum_{t=1}^{\infty} \frac{1}{t^s} \sum_{d=1}^{\infty} \frac{1}{d^{s-k}} = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{t \cdot d = n} d^k,$$

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

Quadratfreie Zahlen:

Die natürliche Zahl n heißt *quadratfrei*, wenn n keinen quadratischen Teiler, der größer als 1 ist, enthält. Eine quadratfreie Zahl wird durch $|\mu(n)|$ beschrieben, denn es

ist

$$|\mu(n)| = \begin{cases} 1 & \text{für } n \text{ quadratfrei,} \\ 0 & \text{sonst.} \end{cases}$$

Da $|\mu(n)|$ multiplikativ ist, verwenden wir Satz 5.7 für $s > 1$.

$$\sum_{n=1}^{\infty} \frac{|\mu(n)|}{n^s} = \prod_p (1 + p^{-s}) = \prod_p \frac{1 - p^{-2s}}{1 - p^{-s}},$$

$$\sum_{n=1}^{\infty} \frac{|\mu(n)|}{n^s} = \frac{\zeta(s)}{\zeta(2s)}.$$

Die Eulersche φ-Funktion:

Aus $\varphi(n) = n * \mu(n)$ ergibt sich für $s > 2$

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{t \cdot d = n} t\mu(d) = \sum_{t=1}^{\infty} \frac{1}{t^{s-1}} \sum_{d=1}^{\infty} \frac{\mu(d)}{d^s},$$

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

Die Primfaktoren von n:

Für die Anzahl $\omega(n)$ der verschiedenen Primfaktoren von n gilt $\omega(n_1 n_2) = \omega(n_1) + \omega(n_2)$ unter der Voraussetzung $(n_1, n_2) = 1$. Daher ist $2^{\omega(n)}$ multiplikativ, und nach Satz 5.7 ist für $s > 1$

$$\sum_{n=1}^{\infty} \frac{2^{\omega(n)}}{n^s} = \prod_p \left(\sum_{\nu=0}^{\infty} \frac{2^{\omega(p^\nu)}}{p^{\nu s}} \right) = \prod_p \left(1 + 2 \sum_{\nu=1}^{\infty} \frac{1}{p^{\nu s}} \right)$$

$$= \prod_p \frac{1 + p^{-s}}{1 - p^{-s}} = \prod_p \frac{1 - p^{-2s}}{(1 - p^{-s})^2},$$

$$\sum_{n=1}^{\infty} \frac{2^{\omega(n)}}{n^s} = \frac{\zeta^2(s)}{\zeta(2s)}.$$

Die Mangoldtsche Funktion:

Aus $\Lambda(n) = \log p$ für $n = p^\nu$ und $\Lambda(n) = 0$ sonst folgt für $s > 1$

$$\sum_{n=2}^{\infty} \frac{\Lambda(n)}{\log n} \cdot \frac{1}{n^s} = \sum_p \sum_{\nu=1}^{\infty} \frac{1}{\nu} \cdot \frac{1}{p^{\nu s}} = -\sum_p \log (1 - p^{-s}),$$

$$\sum_{n=2}^{\infty} \frac{\Lambda(n)}{\log n} \cdot \frac{1}{n^s} = \log \zeta(s).$$

In der Analysis lernt man, daß eine solche Reihe gliedweise differenziert werden darf:

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

5.3. Abschätzungen von Summen

Da in den folgenden Abschnitten in starkem Maße Summen abgeschätzt werden müssen, sollen hier die dazu benötigten Hilfsmittel bereitgestellt werden. Wir führen zunächst eine auf E. LANDAU (1877—1938) zurückgehende, vereinfachende Schreibweise für Abschätzungen ein. Die dabei auftretenden Funktionen können wir uns recht allgemein vorstellen. Es soll das Verhalten einer reell- oder komplexwertigen Funktion $f(x)$ beschrieben werden, wenn x gegen irgendeinen Wert x_0, gleichgültig ob endlich oder unendlich, strebt. Eine Aussage über das Verhalten von $f(x)$ für $x \to x_0$ beinhaltet eine Aussage über alle x, die dem Definitionsbereich von $f(x)$ entnommen sind und hinreichend nahe bei x_0 liegen. Letzteres bedeutet genauer für endliches x_0, daß es ein x_1 gibt, so daß die Aussage für $0 < |x - x_0| < x_1$ zutrifft. Entsprechend gibt es für $x_0 = \infty$ dann ein x_1, so daß für $x > x_1$ die Aussage getroffen wird. In diesem Sinne ist die folgende Definition zu verstehen.

Definition 5.9. Die Funktion $f(x)$ heißt ein *Groß-O* der Funktion $g(x)$ für $x \to x_0$, geschrieben $f(x) = O\big(g(x)\big)$ $(x \to x_0)$, wenn es eine von x unabhängige Konstante $C > 0$ gibt mit $|f(x)| \leqq C\,|g(x)|$ für $x \to x_0$.

Die Funktion $f(x)$ heißt ein *Klein-o* der Funktion $g(x)$ für $x \to x_0$, geschrieben $f(x) = o\big(g(x)\big)$ $(x \to x_0)$, wenn

$$\lim_{x \to x_0} \frac{f(x)}{g(x)} = 0$$

ist.

Wenn die Angabe $x \to x_0$ aus dem Zusammenhang klar ist, kann sie auch weggelassen werden. Eine Gleichung $f(x) = h(x) + O\big(g(x)\big)$ meint $f(x) - h(x) = O\big(g(x)\big)$. Analog wird bei o vorgegangen.

Definition 5.10. Die Funktionen $f(x)$, $g(x)$ heißen für $x \to x_0$ *asymptotisch gleich*, geschrieben $f(x) \sim g(x)$ $(x \to x_0)$, wenn

$$\lim_{x \to x_0} \frac{f(x)}{g(x)} = 1$$

ist.

Die hier benötigten Abschätzungen von Summen basieren sämtlich auf der Abelschen Identität und der Euler-Maclaurinschen Summenformel.

Satz 5.8 (Abelsche Identität). *Sind $f(n)$ und $g(n)$ zahlentheoretische Funktionen, $G(x) = \sum\limits_{n \leqq x} g(n)$ für $x \geqq 1$, $G(x) = 0$ für $x < 1$, so gilt für $0 \leqq a < b$*

$$\sum_{a < n \leqq b} f(n)\, g(n) = f([b])\, G(b) - f([a] + 1)\, G(a) + \sum_{a < n \leqq b-1} \{f(n) - f(n+1)\}\, G(n). \tag{3}$$

Ist überdies $f(t)$ im gesamten Intervall $[\![a, b]\!]$ erklärt und stetig und in $]\!]a, b[\![$ einmal stetig differenzierbar, so gilt

$$\sum_{a < n \leqq b} f(n)\, g(n) = f(b)\, G(b) - f(a)\, G(a) - \int_a^b f'(t)\, G(t)\, dt. \tag{4}$$

Beweis.

$$\sum_{a<n\leqq b} f(n)\,g(n) = \sum_{n=[a]+1}^{[b]} f(n)\,\{G(n) - G(n-1)\}$$

$$= \sum_{n=[a]+1}^{[b]} f(n)\,G(n) - \sum_{n=[a]}^{[b]-1} f(n+1)\,G(n)$$

$$= f([b])\,G(b) - f([a]+1)\,G(a) + \sum_{a<n\leqq b-1} \{f(n) - f(n+1)\}\,G(n).$$

Das ist die Formel (3). Ist noch die Zusatzvoraussetzung erfüllt, so folgt

$$\sum_{a<n\leqq b} f(n)\,g(n) = f([b])\,G(b) - f([a]+1)\,G(a) - \sum_{a<n\leqq b-1} G(n) \int_n^{n+1} f'(t)\,dt$$

$$= f([b])\,G(b) - f([a]+1)\,G(a) - \int_{[a]+1}^{[b]} f'(t)\,G(t)\,dt$$

$$= f(b)\,G(b) - f(a)\,G(a) - \int_a^b f'(t)\,G(t)\,dt$$

und damit Formel (4).

Satz 5.9 (Euler-Maclaurinsche Summenformel). *Ist $f(t)$ in $[\![a,b]\!]$ $(0 \leqq a < b)$ stetig und in $]\!]a,b[\![$ einmal stetig differenzierbar und bezeichnet $\psi(t) = t - [t] - 1/2$, so gilt*

$$\sum_{a<n\leqq b} f(n) = \int_a^b f(t)\,dt - \psi(b)\,f(b) + \psi(a)\,f(a) + \int_a^b f'(t)\,\psi(t)\,dt. \tag{5}$$

Beweis. Setzt man in (4) $g(n) = 1$, so wird

$$\sum_{a<n\leqq b} f(n) = [b]\,f(b) - [a]\,f(a) - \int_a^b f'(t)\,[t]\,dt.$$

Verwendet man hierin die Identität

$$\int_a^b f'(t)\left(t - \frac{1}{2}\right)dt = f(b)\left(b - \frac{1}{2}\right) - f(a)\left(a - \frac{1}{2}\right) - \int_a^b f(t)\,dt,$$

so ergibt sich unmittelbar (5).

Ist $f(t)$ in $[\![a,b]\!]$ mehrmals differenzierbar, so kann man die Formel (5) noch weiter entwickeln. Nehmen wir $f(t)$ in $[\![a,b]\!]$ k-mal und in $]\!]a,b[\![$ $(k+1)$-mal stetig differenzierbar an und definieren

$$\psi_\nu(t) = \int_0^t \psi_{\nu-1}(t)\,dt \qquad (\nu = 1, 2, \ldots), \qquad \psi_0(t) = \psi(t),$$

so erhalten wir durch fortgesetzte partielle Integration des zweiten Integrals in (5)

$$\sum_{a<n\leq b} f(n) = \int_a^b f(t)\,dt + \sum_{\nu=0}^{k} (-1)^\nu \{\psi_\nu(a) f^{(\nu)}(a) - \psi_\nu(b) f^{(\nu)}(b)\}$$
$$+ (-1)^k \int_a^b f^{(k+1)}(t)\,\psi_k(t)\,dt. \tag{6}$$

An Hand einiger wichtiger Beispiele, die alle später gebraucht werden, soll demonstriert werden, wie die Euler-Maclaurinsche Summenformel für die Abschätzung von Summen ausgenutzt werden kann. Alle Formeln verstehen sich für $x \to \infty$, so daß dies im einzelnen nicht vermerkt wird.

1. Abschätzung von $\sum_{1\leq n\leq x} n^\alpha$, $\alpha \geqq 0$.

In (5) setzen wir $f(n) = n^\alpha$, $a = 0$, $b = x$. Dann erhalten wir

$$\sum_{1\leq n\leq x} n^\alpha = \int_0^x t^\alpha\,dt - \psi(x)\,x^\alpha - \frac{1}{2} f(0) + \alpha \int_0^x t^{\alpha-1}\,\psi(t)\,dt,$$

wobei für $\alpha = 0$ das letzte Integral entfällt. Wegen $|\psi(t)| \leqq 1/2$ ist

$$\left|\alpha \int_0^x t^{\alpha-1}\,\psi(t)\,dt\right| \leqq \frac{\alpha}{2} \int_0^x t^{\alpha-1}\,dt = \frac{1}{2}\,x^\alpha$$

und daher

$$\sum_{1\leq n\leq x} n^\alpha = \frac{x^{\alpha+1}}{\alpha+1} + O(x^\alpha). \tag{7}$$

2. Abschätzung von $\sum_{1\leq n\leq x} \frac{1}{n}$.

Wir verwenden die Formel (6) mit $k = 1$ und setzen $f(n) = 1/n$, $a = 1$, $b = x$.

$$\sum_{1<n\leq x} \frac{1}{n} = \int_1^x \frac{dt}{t} - \frac{1}{2} - \frac{\psi(x)}{x} + \frac{\psi_1(1)}{1} - \frac{\psi_1(x)}{x^2} - 2\int_1^x \frac{\psi_1(t)}{t^3}\,dt.$$

$\psi_1(t)$ errechnet sich zu

$$\psi_1(t) = \frac{1}{2}\,(t - [t])^2 - \frac{1}{2}\,(t - [t]).$$

Daher ist $\psi_1(1) = 0$ und $\psi_1(t) = O(1)$ für $t \to \infty$, und wir erhalten für das letzte Integral

$$\int_1^x \frac{\psi_1(t)}{t^3}\,dt = \int_1^\infty \frac{\psi_1(t)}{t^3}\,dt - \int_x^\infty \frac{\psi_1(t)}{t^3}\,dt = \int_1^\infty \frac{\psi_1(t)}{t^3}\,dt + O\left(\frac{1}{x^2}\right).$$

Die Zahl

$$C := \frac{1}{2} - 2\int_1^\infty \frac{\psi_1(t)}{t^3}\,dt$$

wird als *Eulersche Konstante* bezeichnet. Mit ihrer Verwendung erhalten wir

$$\sum_{1\leqq n\leqq x}\frac{1}{n} = \log x + C - \frac{\psi(x)}{x} + O\left(\frac{1}{x^2}\right). \tag{8}$$

3. Abschätzung von $\sum_{1\leqq n\leqq x}\frac{1}{n^s}$, $\quad s>1$.

Wir beginnen mit der Anwendung von (5) und setzen $f(n) = 1/n^s$, $a = 1$, $b = x$. Dies ergibt

$$\sum_{1<n\leqq x}\frac{1}{n^s} = \int_1^x \frac{dt}{t^s} - \frac{1}{2} - \frac{\psi(x)}{x^s} - s\int_1^x \frac{\psi(t)}{t^{s+1}}\,dt,$$

$$\sum_{1\leqq n\leqq x}\frac{1}{n^s} = \frac{1}{s-1} + \frac{1}{2} - \frac{x^{1-s}}{s-1} - s\int_1^x \frac{\psi(t)}{t^{s+1}}\,dt + O\left(\frac{1}{x^s}\right).$$

Wegen $s>1$ können wir in dieser Gleichung den Grenzübergang $x\to\infty$ vollziehen und erhalten mit

$$\zeta(s) = \frac{1}{s-1} + \frac{1}{2} - s\int_1^\infty \frac{\psi(t)}{t^{s+1}}\,dt \tag{9}$$

eine *Integraldarstellung der Riemannschen Zetafunktion*. Da sich das Integral aber schon für $s>0$ als konvergent erweist, kann man dies zum Anlaß nehmen, $\zeta(s)$ für $s>0$, $s\neq 1$, durch (9) zu definieren. Verwenden wir also (9), so erhalten wir

$$\sum_{1\leqq n\leqq x}\frac{1}{n^s} = \zeta(s) - \frac{x^{1-s}}{s-1} + O\left(\frac{1}{x^s}\right).$$

Für spätere Anwendungen benötigen wir aber noch eine genauere Formel. Wir benutzen (6) mit $k=1$ und erhalten

$$\sum_{1<n\leqq x}\frac{1}{n^s} = \frac{1}{s-1} - \frac{x^{1-s}}{s-1} - \frac{1}{2} - \frac{\psi(x)}{x^s} - \frac{s\psi_1(x)}{x^{s+1}} - s(s+1)\int_1^x \frac{\psi_1(t)}{t^{s+2}}\,dt.$$

Aus (9) folgt

$$\zeta(s) = \frac{1}{s-1} + \frac{1}{2} - s(s+1)\int_1^\infty \frac{\psi_1(t)}{t^{s+2}}\,dt.$$

Damit erhalten wir

$$\sum_{1\leqq n\leqq x}\frac{1}{n^s}=\zeta(s)-\frac{x^{1-s}}{s-1}-\frac{\psi(x)}{x^s}+O\left(\frac{1}{x^{s+1}}\right). \tag{10}$$

4. Abschätzung von $\sum_{1\leqq n\leqq x}\frac{1}{n^s}$, $0<s<1$.

Bei Benutzung der Definition (9) ändert sich an den Rechnungen von Beispiel 3 nichts, so daß (10) auch in diesem Fall richtig ist.

5. Die Stirlingsche Formel.

In (6) setzen wir $k=1, f(n)=\log n, a=1, b=m$. Dann wird

$$\log(m!)=\sum_{n=1}^{m}\log n=\int_1^m \log t+\frac{1}{2}\log m+\int_1^m\frac{\psi_1(t)}{t^2}\,dt$$

$$=m\log m-m+1+\frac{1}{2}\log m+\int_1^\infty\frac{\psi_1(t)}{t^2}\,dt+O\left(\frac{1}{m}\right).$$

Ohne Beweis sei

$$\int_1^\infty\frac{\psi_1(t)}{t^2}\,dt=\frac{1}{2}\log(2\pi)-1$$

mitgeteilt. Damit erhalten wir

$$\log(m!)=m\log m-m+\frac{1}{2}\log(2\pi m)+O\left(\frac{1}{m}\right) \tag{11}$$

und daraus die Stirlingsche Formel

$$m!=m^m\sqrt{2\pi m}\;e^{-m}\left\{1+O\left(\frac{1}{m}\right)\right\}.$$

5.4. Die Primzahlfunktion

5.4.1. Der Euklidische Beweis der Unendlichkeit der Menge der Primzahlen

Im Beweis zu Satz 1.2 haben wir die Euklidische Beweisidee für die Unendlichkeit von Primzahlmengen kennengelernt. Sie ist zwar überaus einfach, aber nicht sehr ausbaufähig. Wir werden sie in diesem Abschnitt noch an zwei Beispielen demonstrieren, später aber zugkräftigere Methoden für tiefere Ergebnisse heranziehen.

Satz 5.10. *Für jedes Polynom*

$$f(x)=a_0+a_1x+\cdots+a_rx^r$$

mit ganzzahligen Koeffizienten und $a_r > 0$, $r \geqq 1$, existieren unendlich viele Primzahlen p, so daß $p \mid f(n)$ mit geeigneten $n \in \mathbf{N}$.

Beweis. Für $a_0 = 0$ ist die Behauptung nach Satz 1.2 und $p \mid f(p)$ klar. Jetzt sei $a_0 \neq 0$. Wir nehmen an, es gibt nur endlich viele Primteiler $p_1, p_2, \ldots, p_\nu$ der Folge $\{f(n)\}$ mit $p_i \nmid a_0$ $(i = 1, 2, \ldots, \nu)$ und bilden die Zahlen $n = 2^k p_1 p_2 \cdot \cdots \cdot p_\nu$ und

$$f(a_0 2^n) = a_0(1 + a_1 a_0 n + a_2 a_0^3 n^2 + \cdots + a_r a_0^{2r-1} n^r) = a_0 m.$$

Da für $x \to \infty$ auch $f(x) \to \infty$ geht, ist $m > 1$ für hinreichend großes k. Folglich gibt es eine Primzahl p mit den Eigenschaften $p \mid m$, $p \nmid a_0$ und $p \nmid n$. Das steht im Widerspruch zur Annahme.

Das zweite Beispiel bezieht sich auf *Primzahlen in arithmetischen Progressionen.* Unter einer arithmetischen Progression versteht man eine Folge natürlicher Zahlen der Gestalt $kn + a$, in der k, a feste natürliche Zahlen mit $(k, a) = 1$ sind und n die Folge der natürlichen Zahlen durchläuft. P. G. L. Dirichlet bewies 1837, daß jede arithmetische Progression unendlich viele Primzahlen enthält. Dieses Ergebnis kann im allgemeinen nicht mit der Euklidischen Beweisidee erreicht werden. In einigen Spezialfällen kommt man mit ihr noch zum Zuge. Es soll dies im Fall der primen Restklassen modulo 8 dargestellt werden.

Satz 5.11. *Es gibt unendlich viele Primzahlen der Gestalt $p \equiv a$ (8) mit $a = 1, 3, 5, 7$.*

Wir führen die Beweise für $a = 1$ und $a = 3, 5, 7$ getrennt.

Beweis für $a = 1$. Wir zeigen zunächst, daß jeder Primteiler des Polynoms $f(x) = x^4 + 1$, $x \in \mathbf{Z}$, $x \neq 0, \pm 1$, von der Gestalt $p \equiv 1$ (8) ist. Aus $x^4 + 1 \equiv 0$ (p) folgt $(x^2)^2 \equiv -1$ (p), so daß notwendigerweise

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$$

sein muß. Das bedeutet $p \equiv 1$ (4) oder, was dasselbe ist, $p \equiv 1, 5$ (8). Aus $x^4 + 1 \equiv 0$ (p) folgt auch $(x^2 + 1)^2 - 2x^2 \equiv 0$ (p) und

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

Also $p \equiv 1, 7$ (8). Beide Ergebnisse zusammen lassen nur $p \equiv 1$ (8) zu. Also ist jeder Primteiler von $f(x) = x^4 + 1$ von der Gestalt $p \equiv 1$ (8), und nach Satz 5.10 gibt es unendlich viele derartige Primteiler.

Beweis für $a = 3, 5, 7$. Wir bilden die Polynome

$$f_3(x) = (8x + 1)^2 + 2 \equiv 3 \quad (8),$$

$$f_5(x) = \frac{1}{2}\{(8x + 3)^2 + 1\} \equiv 5 \quad (8),$$

$$f_7(x) = (4x + 3)^2 - 2 \equiv 7 \quad (8)$$

und führen den Beweis für die drei Fälle gemeinsam in drei Schritten.

1. *Schritt.* Es wird gezeigt, daß jeder Primteiler p von $f_a(x)$ von der Gestalt $p \equiv 1$ (8) oder $p \equiv a$ (8) ist.

a) $a = 3$: $(8x+1)^2 + 2 \equiv 0 \quad (p) \Rightarrow \left(\frac{-2}{p}\right) = (-1)^{\frac{p-1}{2} + \frac{p^2-1}{8}} = 1$

$$\Rightarrow \frac{(p-1)(p+5)}{8} \equiv 0 \quad (2)$$

$$\Rightarrow p \equiv 1, 3 \quad (8).$$

b) $a = 5$: $\frac{1}{2}\{(8x+3)^2 + 1\} \equiv 0 \quad (p) \Rightarrow \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$

$$\Rightarrow p \equiv 1, 5 \quad (8).$$

c) $a = 7$: $(4x+3)^2 - 2 \equiv 0 \quad (p) \Rightarrow \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1$

$$\Rightarrow p \equiv 1, 7 \quad (8).$$

2. *Schritt.* Es wird gezeigt, daß es für $x \in \mathbf{Z}$ ($x \neq -1$ für $a = 7$) eine Primzahl $p \equiv a$ (8) mit $p \mid f_a(x)$ gibt.

Alle Primteiler von $f_a(x)$ sind nach dem ersten Schritt von der Gestalt $p \equiv 1, a$ (8). Würde $f_a(x)$ nur Primteiler $p \equiv 1$ (8) besitzen, so müßte $f_a(x) \equiv 1$ (8) sein im Widerspruch zu $f_a(x) \equiv a$ (8).

3. *Schritt.* Annahme: Es gibt nur endlich viele Primzahlen $p \equiv a$ (8). Wir notieren sie uns durch $a, p_1, p_2, \ldots, p_r$ und bilden $P = p_1 p_2 \cdot \cdots \cdot p_r$. Die Zahl $f_a(P^{a-1})$ enthält nach der Feststellung im zweiten Schritt wenigstens einen Primteiler $p \equiv a$ (8). Dieser ist von allen p_i verschieden. Denn es ist $f_a(P^{a-1}) \equiv a \quad (p_i)$, und da $(a, p_i) = 1$ vorausgesetzt wurde, ist $p_i \nmid f_a(P^{a-1})$. Der Primteiler p muß auch von a verschieden sein, da nach dem Satz von FERMAT-EULER $f_a(P^{a-1}) \equiv f_a(1) \not\equiv 0 \quad (a)$ ist. Das ist aber ein Widerspruch zur Annahme.

5.4.2. Einfache Abschätzungen der Primzahlfunktionen

Definition 5.11. Für positive reelle Zahlen x bezeichne $\pi(x)$ die *Anzahl der Primzahlen* kleiner oder gleich x.

Aus dem Euklidischen Beweis haben wir für die n-te Primzahl p_n in Kapitel 1 die Abschätzung

$$p_n \leqq 2^{2^{n-1}}$$

gefunden. Hieraus folgt eine Abschätzung von $\pi(x)$ nach unten. Für jedes $x \geqq 2$ gibt

es eine nicht-negative, ganze Zahl n mit

$$2^{2^n} \leqq x < 2^{2^{n+1}}.$$

Daraus folgt

$$\pi(x) \geqq \pi(2^{2^n}) \geqq \pi(p_{n+1}) = n + 1 > \frac{1}{\log 2}(\log\log x - \log\log 2),$$

$$\pi(x) > \frac{\log\log x}{\log 2}.$$

Eine Verbesserung dieser Abschätzung können wir erzielen, wenn wir uns einer auf L. Euler zurückgehenden Beweisidee zum Satz 1.2 bedienen. Nehmen wir wieder an, es gibt nur endlich viele Primzahlen $p_1, p_2, \ldots, p_n$. Dann ist auch das Produkt

$$\prod_{i=1}^{n}\left(1 - \frac{1}{p_i}\right)^{-1}$$

endlich. Andererseits ist aber

$$\prod_{i=1}^{n}\left(1 - \frac{1}{p_i}\right)^{-1} = \prod_{i=1}^{n}\left(1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \cdots\right) = \sum \frac{1}{m}.$$

In der Summe müssen auf Grund der eindeutigen Primfaktorzerlegung alle natürlichen Zahlen m erscheinen. Dann handelt es sich aber um die divergente harmonische Reihe.

Unter Verwendung dieser Idee zeigen wir, daß die Summe über die Reziproken der Primzahlen divergent ist.

Satz 5.12. *Das Produkt* $\prod(1 - 1/p)$ *und die Summe* $\sum 1/p$, *jeweils erstreckt über alle Primzahlen, sind divergent. Genauer gilt für* $x \geqq 2$

$$\prod_{p \leqq x}\left(1 - \frac{1}{p}\right)^{-1} > \log x, \tag{12}$$

$$\sum_{p \leqq x} \frac{1}{p} > \log\log x - 1. \tag{13}$$

Beweis. Es ist

$$\prod_{p \leqq x}\left(1 - \frac{1}{p}\right)^{-1} = \sum{}' \frac{1}{n},$$

wobei die (konvergente!) Summe über alle diejenigen natürlichen Zahlen n zu erstrecken ist, die aus den Primzahlen $p \leqq x$ gebildet werden. Die Ungleichung (12) folgt nun aus

$$\prod_{p \leqq x}\left(1 - \frac{1}{p}\right)^{-1} \geqq \sum_{n \leqq x} \frac{1}{n} = \sum_{n \leqq x} \int_n^{n+1} \frac{1}{n}\, dt \geqq \int_1^{[x]+1} \frac{dt}{t} = \log([x] + 1) > \log x.$$

Die Ungleichung (13) erhalten wir durch Logarithmieren von (12).

$$\log\log x < -\sum_{p\leqq x}\log\left(1-\frac{1}{p}\right)=\sum_{p\leqq x}\sum_{n=1}^{\infty}\frac{1}{np^n}<\sum_{p\leqq x}\sum_{n=1}^{\infty}\frac{1}{p^n}$$

$$=\sum_{p\leqq x}\frac{1}{p-1}=\sum_{p\leqq x}\frac{1}{p}+\sum_{p\leqq x}\left(\frac{1}{p-1}-\frac{1}{p}\right)$$

$$<\sum_{p\leqq x}\frac{1}{p}+\sum_{n=2}^{\infty}\left(\frac{1}{n-1}-\frac{1}{n}\right)=\sum_{p\leqq x}\frac{1}{p}+1.$$

Aus (12) erhalten wir eine Verbesserung der Abschätzung von $\pi(x)$ nach unten:

$$\log x<\prod_{p\leqq x}\left(1-\frac{1}{p}\right)^{-1}=\prod_{n=1}^{\pi(x)}\left(1-\frac{1}{n+1}\right)^{-1}=\pi(x)+1,$$

$$\pi(x)>\log x-1.$$

Für die n-te Primzahl ergibt sich aus $n=\pi(p_n)>\log p_n-1$:

$$p_n<e^{n+1}.$$

Mit dieser Abschätzung von $\pi(x)$ nach unten wollen wir uns hier begnügen, schärfere Abschätzungen sollen erst in den nächsten Abschnitten besprochen werden. Wir bemühen uns noch um eine möglichst einfache Abschätzung von $\pi(x)$ nach oben. Wir bedienen uns dabei des *Siebes von* ERATOSTHENES (um 200 v. u. Z.), das ein sehr altes Verfahren zur Aufstellung von Primzahltafeln beinhaltet.

Ist x nicht zu groß, so können wir auf folgende Weise alle Primzahlen unterhalb von x bestimmen. Wir schreiben uns alle natürlichen Zahlen n mit $2\leqq n\leqq x$ der Reihe nach auf. Sodann ist die erste auftretende Zahl, die 2, Primzahl. Wir lassen sie stehen, streichen jedoch ihre sämtlichen Vielfachen fort. Die nächste stehengebliebene Zahl, die 3, muß wieder Primzahl sein. Wir belassen die 3, streichen aber wieder alle Vielfachen weg. Indem wir fortfahren, bleiben schließlich genau die Primzahlen unterhalb x stehen. Zu bemerken ist dabei, daß das Verfahren mit dem Streichen der Vielfachen der größten Primzahl $p\leqq\sqrt{x}$ bereits beendet ist, denn die Vielfachen der größeren Primzahlen sind bereits gestrichen. Dies gibt eine Möglichkeit, $\pi(x)$ zu berechnen, falls $\pi(\sqrt{x})$ bekannt ist. Verfährt man etwas modifiziert so, daß man alle natürlichen Zahlen n mit $1\leqq n\leqq x$ aufschreibt und sämtliche Primzahlen unterhalb von $\sqrt{x}$ und ihre Vielfachen streicht, so verbleiben $1+\pi(x)-\pi(\sqrt{x})$ nicht gestrichene Zahlen. Genau diese sind zu allen Primzahlen $p\leqq\sqrt{x}$, also zu $P=\prod_{p\leqq\sqrt{x}}p$ teilerfremd. Daher ist

$$1+\pi(x)-\pi(\sqrt{x})=\sum_{\substack{n\leqq x\\(n,P)=1}}1=\sum_{n\leqq x}\sum_{t\mid(n,P)}\mu(t)$$

$$=\sum_{t\mid P}\mu(t)\sum_{\substack{n\leqq x\\ n\equiv 0\ (t)}}1=\sum_{t\mid P}\mu(t)\sum_{tm\leqq x}1.$$

Daraus ergibt sich

$$\pi(x) = \pi(\sqrt{x}) - 1 + \sum_{t|P} \mu(t) \left[\frac{x}{t}\right].$$

Zur Abschätzung von $\pi(x)$ ändern wir das Verfahren nochmals geringfügig ab. Es sei jetzt $P_y = \prod_{p \leqq y} p$ mit $y \leqq \sqrt{x}$ und

$$N(x) = \sum_{\substack{n \leqq x \\ (n, P_y)=1}} 1 = \sum_{t|P_y} \mu(t) \left[\frac{x}{t}\right].$$

Offensichtlich ist $N(x) \geqq \pi(x) - \pi(y)$, und daher ist für beliebiges $y \leqq \sqrt{x}$

$$\pi(x) \leqq \pi(y) + \sum_{t|P_y} \mu(t) \left[\frac{x}{t}\right].$$

In dieser Ungleichung kommt es nun darauf an, y möglichst so zu wählen, daß die Abschätzung optimal wird. Dazu schätzen wir noch etwas weiter ab.

$$\pi(x) \leqq \pi(y) + \sum_{t|P_y} \mu(t) \frac{x}{t} + \sum_{t|P_y} 1 = \pi(y) + \frac{x}{P_y} \varphi(P_y) + d(P_y)$$

$$= \pi(y) + x \prod_{p \leqq y} \left(1 - \frac{1}{p}\right) + 2^{\pi(y)} < y + \frac{x}{\log y} + 2^y < \frac{x}{\log y} + 2^{y+1}.$$

Setzt man jetzt $y = \log x$, so wird

$$\pi(x) < \frac{x}{\log \log x} + 2^{\log x + 1}.$$

Für $x \geqq e^3$ wird daraus noch

$$\pi(x) < \frac{2x}{\log \log x}.$$

5.4.3. Die Ergebnisse von Čebyšev

Die bisher vorliegenden Abschätzungen von $\pi(x)$ sind außerordentlich ungenau. Erst im Jahre 1850 gelang es P. L. Čebyšev (1821—1894), Abschätzungen nach unten und nach oben von gleicher Qualität zu geben. Diese Ergebnisse sollen jetzt dargelegt werden. Wir beginnen mit der Einführung der Čebyševschen Funktionen $\vartheta(x)$ und $\psi(x)$, wobei $\psi(x)$ nicht mit der in der Euler-Maclaurinschen Summenformel auftretenden Funktion zu verwechseln ist.

Definition 5.12.

$$\vartheta(x) := \sum_{p \leqq x} \log p, \qquad \psi(x) := \sum_{n \leqq x} \Lambda(n).$$

Dabei ist $\vartheta(x) = 0$ für $x < 2$ zu setzen.

Beide Funktionen verhalten sich für $x \to \infty$ in erster Näherung gleich. Dies erkennt man, wenn man $\Lambda(n) = \log p$ für $n = p^r$ und $\Lambda(n) = 0$ sonst verwendet.

$$\psi(x) = \sum_{p^r \leqq x} \log p = \sum_{p \leqq x} \log p + \sum_{p^2 \leqq x} \log p + \cdots$$

$$= \vartheta(x) + \vartheta\left(\sqrt{x}\right) + \cdots = \sum_{m=1}^{\infty} \vartheta(x^{1/m}).$$

Die Reihe ist endlich; sie bricht ab, wenn $x^{1/m} < 2$, das heißt $m > \dfrac{\log x}{\log 2}$ geworden ist. Aus $\vartheta(x) < x \log x$ für $x \geqq 2$ folgt

$$\vartheta(x^{1/m}) < x^{1/m} \log x^{1/m} < \sqrt{x} \log x$$

für $m \geqq 2$. Da die Reihe $O(\log x)$ Glieder hat, ist

$$\sum_{m=2}^{\infty} \vartheta(x^{1/m}) = O\left(\sqrt{x} \log^2 x\right),$$

und es ergibt sich:

Satz 5.13. $\psi(x) = \vartheta(x) + O\left(\sqrt{x} \log^2 x\right)$.

Satz 5.14. *Für $x \geqq 2$ existieren positive Konstanten A_1, A_2, B_1, B_2 mit*

$$A_1 x < \vartheta(x) < B_1 x, \qquad A_2 x < \psi(x) < B_2 x.$$

Beweis. Wegen Satz 5.13 genügt es, die Behauptung für $\psi(x)$ zu beweisen. Unter Benutzung von $1 * \Lambda(n) = \log n$ und der Stirlingschen Formel ergibt sich

$$\sum_{n \leqq x} \psi\left(\frac{x}{n}\right) = \sum_{dn \leqq x} \Lambda(d) = \sum_{n \leqq x} \sum_{d \mid n} \Lambda(d) = \sum_{m \leqq x} \log m \tag{14}$$

$$= x \log x - x + O(\log x)$$

und

$$f(x) := \sum_{n \leqq x} \psi\left(\frac{x}{n}\right) - 2 \sum_{n \leqq x/2} \psi\left(\frac{x}{2n}\right) = x \log 2 + O(\log x).$$

Da die Funktion $\psi(x)$ monton wachsend ist, folgt

$$f(x) = \psi(x) - \sum_{m \geqq 1} \left(\psi\left(\frac{x}{2m}\right) - \psi\left(\frac{x}{2m+1}\right)\right) \leqq \psi(x),$$

so daß die Existenz einer Konstanten A_2 mit $A_2 x < \psi(x)$ sofort klar ist.

Für den Beweis der zweiten Ungleichung vermerken wir

$$f(x) = \psi(x) - \psi\left(\frac{x}{2}\right) + \sum_{m \geqq 2} \left(\psi\left(\frac{x}{2m-1}\right) - \psi\left(\frac{x}{2m}\right)\right) \geqq \psi(x) - \psi\left(\frac{x}{2}\right).$$

Also gibt es eine Konstante B mit

$$\psi(x) < Bx + \psi\left(\frac{x}{2}\right),$$

und sukzessive Anwendung dieser Ungleichung liefert

$$\psi(x) < Bx\left(1+\frac{1}{2}\right)+\psi\left(\frac{x}{4}\right) < \cdots < Bx\sum_{\nu=0}^{n-1}\frac{1}{2^\nu}+\psi\left(\frac{x}{2^n}\right)$$

$$< Bx\sum_{\nu=0}^{\infty}\frac{1}{2^\nu} = B_2 x.$$

Damit ist der Satz bewiesen.

Nun sind wir in der Lage, *das erste Čebyševsche Ergebnis* zu beweisen.

Satz 5.15 (ČEBYŠEV). *Für $x \geqq 2$ gibt es positive Konstanten A, B mit*

$$A\frac{x}{\log x} < \pi(x) < B\frac{x}{\log x}.$$

Beweis. Mit Hilfe von Satz 5.14 erhalten wir leicht

$$\pi(x) \geqq \sum_{p\leqq x}\frac{\log p}{\log x} = \frac{\vartheta(x)}{\log x} > A\frac{x}{\log x}$$

und

$$\pi(x) - \pi\left(\sqrt{x}\right) \leqq \sum_{\sqrt{x}<p\leqq x}\frac{2\log p}{\log x} \leqq \frac{2\vartheta(x)}{\log x},$$

$$\pi(x) \leqq \sqrt{x} + \frac{2\vartheta(x)}{\log x} < B\frac{x}{\log x}.$$

Die in diesem Satz erhaltene Abschätzung wurde wesentlich durch Zurückführung von $\pi(x)$ auf $\vartheta(x)$ erzielt. Dieser Zusammenhang kann nun noch etwas schärfer gefaßt werden.

Satz 5.16. *Für $x \to \infty$ gilt*

$$\pi(x) \sim \frac{\vartheta(x)}{\log x} \sim \frac{\psi(x)}{\log x}.$$

Beweis. Auf Grund des Satzes 5.13 genügt es, die Behauptung für $\vartheta(x)$ nachzuweisen. Wir benutzen die Formel (4) und setzen dort $a = 1$, $b = x$, $f(n) = \log n$, $g(n) = 1$ für $n = p$, $g(n) = 0$ sonst. Dann ist

$$\vartheta(x) = \sum_{p\leqq x}\log p = \sum_{1<n\leqq x} g(n)\log n = \pi(x)\log x - \int_1^x \frac{\pi(t)}{t}\,dt.$$

Aus $\pi(t) = 0$ für $t < 2$ und $\pi(t) = O(t/\log t)$ für $t \geqq 2$ folgt für das Integral

$$\int_1^x \frac{\pi(t)}{t}\,dt = \int_2^{\sqrt{x}}\frac{\pi(t)}{t}\,dt + \int_{\sqrt{x}}^x \frac{\pi(t)}{t}\,dt = O\left(\sqrt{x}\right) + O\left(\frac{x}{\log x}\right) = O\left(\frac{x}{\log x}\right).$$

Damit ist

$$\frac{\vartheta(x)}{\pi(x)\log x} = 1 + O\left(\frac{1}{\log x}\right),$$

woraus die Behauptung folgt.

Satz 5.17. *Für $x \to \infty$ gilt*

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

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

Beweis. Bei Benutzung von (14) ist

$$\sum_{n\leq x} \frac{\Lambda(n)}{n} = \frac{1}{x}\sum_{n\leq x}\left[\frac{x}{n}\right]\Lambda(n) + O\left(\frac{\psi(x)}{x}\right) = \frac{1}{x}\sum_{dn\leq x}\Lambda(n) + O(1)$$

$$= \frac{1}{x}\sum_{d\leq x}\psi\left(\frac{x}{d}\right) + O(1) = \log x + O(1).$$

Die zweite Behauptung folgt aus

$$\sum_{n\leq x}\frac{\Lambda(n)}{n} - \sum_{p\leq x}\frac{\log p}{p} = \sum_{\substack{p^m\leq x\\ m\geq 2}}\frac{\log p}{p^m} < \sum_p \log p \sum_{m=2}^{\infty}\frac{1}{p^m} = \sum_p \frac{\log p}{p(p-1)} = O(1).$$

Aus diesem Satz können wir eine Verschärfung des Satzes 5.12 folgern.

Satz 5.18. *Es gibt zwei Konstanten B und C, so daß für $x \to \infty$ gilt*

$$\sum_{p\leq x}\frac{1}{p} = \log\log x + B + O\left(\frac{1}{\log x}\right), \tag{15}$$

$$\prod_{p\leq x}\left(1-\frac{1}{p}\right)^{-1} \sim e^C \log x. \tag{16}$$

Ohne Beweis sei mitgeteilt, daß es sich bei C um die *Eulersche Konstante* handelt.

Beweis. Nach Satz 5.17 ist

$$\sum_{p\leq x}\frac{\log p}{p} = \log x + r(x)$$

mit $r(x) = O(1)$. Von dieser Summe wird der Übergang zu $\sum 1/p$ mit Hilfe des Integrals

$$\int_2^x \sum_{p\leq t}\frac{\log p}{p}\frac{dt}{t\log^2 t} = \sum_{p\leq x}\frac{\log p}{p}\int_p^x \frac{dt}{t\log^2 t} = \sum_{p\leq x}\frac{\log p}{p}\left(\frac{1}{\log p} - \frac{1}{\log x}\right)$$

vollzogen. Wir erhalten

$$\sum_{p\leqq x}\frac{1}{p}=\frac{1}{\log x}\sum_{p\leqq x}\frac{\log p}{p}+\int_2^x\sum_{p\leqq t}\frac{\log p}{p}\frac{dt}{t\log^2 t}$$

$$=1+\int_2^x\frac{dt}{t\log t}+\int_2^x\frac{r(t)}{t\log^2 t}\,dt+O\left(\frac{1}{\log x}\right)$$

$$=1+\log\log x-\log\log 2+\int_2^\infty\frac{r(t)}{t\log^2 t}\,dt+O\left(\frac{1}{\log x}\right).$$

Das ist (15) mit

$$B=1-\log\log 2+\int_2^\infty\frac{r(t)}{t\log^2 t}\,dt.$$

Formel (16) leiten wir aus (15) ab. Zunächst stellen wir fest, daß auf Grund der Ungleichung

$$0<-\log\left(1-\frac{1}{p}\right)-\frac{1}{p}=\sum_{n=2}^\infty\frac{1}{np^n}<\frac{1}{2}\sum_{n=2}^\infty\frac{1}{p^n}=\frac{1}{2p(p-1)}$$

und der Konvergenz der Reihe

$$\sum_p\frac{1}{p(p-1)}$$

auch die Reihe

$$\sum_p\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right)$$

konvergiert. Daher ist

$$\log\prod_{p\leqq x}\left(1-\frac{1}{p}\right)^{-1}=-\sum_{p\leqq x}\log\left(1-\frac{1}{p}\right)=\sum_{p\leqq x}\frac{1}{p}-\sum_{p\leqq x}\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right)$$

$$=\log\log x+C+o(1)$$

mit

$$C=B-\sum_p\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right).$$

Das bedeutet

$$\prod_{p\leqq x}\left(1-\frac{1}{p}\right)^{-1}=e^{C+o(1)}\log x\sim e^C\log x.$$

Nun gelangen wir zu *Čebyševs zweitem Ergebnis.*

Satz 5.19. *Wenn der Grenzwert*

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = c$$

existiert, dann muß $c = 1$ *sein.*

Beweis. In Anwendung von (4) erhalten wir

$$\sum_{p\leqq x} \frac{1}{p} = \frac{\pi(x)}{x} + \int_2^x \frac{\pi(t)}{t^2}\,dt.$$

Die Voraussetzung des Satzes besagt

$$\pi(x) = c\,\frac{x}{\log x} + \varrho(x), \qquad \varrho(x) = o\left(\frac{x}{\log x}\right).$$

Daher ergibt sich

$$\sum_{p\leqq x} \frac{1}{p} = \frac{c}{\log x} + \int_2^x \frac{c}{t\log t}\,dt + \int_2^x \frac{\varrho(t)}{t^2}\,dt + o\left(\frac{1}{\log x}\right)$$

$$= c\log\log x + \int_2^x \frac{\varrho(t)}{t^2}\,dt + O(1).$$

Zur Abschätzung des Integrals bemerken wir, daß aus $\varrho(x) = o\left(\frac{x}{\log x}\right)$ folgt, daß es zu jedem $\varepsilon > 0$ ein x_0 gibt mit $|\varrho(x)| < \varepsilon\,\frac{x}{\log x}$ für $x > x_0$. So finden wir

$$\left|\int_2^x \frac{\varrho(t)}{t^2}\,dt\right| \leqq \left|\int_2^{x_0} \frac{\varrho(t)}{t^2}\,dt\right| + \varepsilon\int_{x_0}^x \frac{dt}{t\log t} < a(\varepsilon) + \varepsilon\log\log x$$

$$< 2\varepsilon\log\log x$$

für $x > x_1(\varepsilon)$.

Vergleichen wir nun das Ergebnis

$$\sum_{p\leqq x} \frac{1}{p} = c\log\log x + o(\log\log x)$$

mit (15), so sehen wir, daß $c = 1$ sein muß.

Mit den Sätzen 5.15 und 5.19 erzielte P. L. Čebyšev zu seiner Zeit einen wesentlichen Fortschritt in der Primzahltheorie. Seine Ergebnisse waren numerisch, vor allem durch C. F. Gauss und A. M. Legendre, vorbereitet. Sie sprachen die Vermutung

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$$

aus. Aber der Nachweis der Existenz dieses Grenzwertes gelang nicht. Erst etwa 50 Jahre später konnten unabhängig voneinander im selben Jahr 1896 J. HADAMARD (1865—1962) und C. DE LA VALLÉE-POUSSIN (1866—1962) mit funktionentheoretischen Hilfsmitteln den Primzahlsatz

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

beweisen. Lange Zeit wurde die Ansicht vertreten, daß es sich hierbei um einen Satz der Zahlentheorie handelt, der sich den elementaren Methoden entzieht. Um so überraschender war es, daß im Jahre 1949 unabhängig voneinander P. ERDÖS und A. SELBERG einen elementaren Beweis veröffentlichten. Inzwischen existiert eine Reihe von Beweisvarianten. Eine von E. M. WRIGHT gegebene und in [7] dargestellte Variante soll im übernächsten Abschnitt vorgestellt werden. Sie gründet sich — wie auch andere Varianten — auf die Selbergsche Formel und die daraus abgeleitete Selbergsche Ungleichung, die im nächsten Abschnitt behandelt werden sollen.

Es sei noch erwähnt, daß aus dem Primzahlsatz eine *asymptotische Formel für die n-te Primzahl* folgt. Setzt man nämlich $x = p_n$, so ist für $n \to \infty$

$$n \sim \frac{p_n}{\log p_n}.$$

Hieraus kann man

$$\log n \sim \log p_n - \log\log p_n \sim \log p_n$$

ablesen. Folglich ist

$$p_n \sim n \log n.$$

5.4.4. Die Selbergsche Formel

In Vorbereitung der Selbergschen Formel beginnen wir mit zwei Hilfssätzen.

Hilfssatz 5.1. *Für $k \geqq 0$ und $x \to \infty$ gilt*

$$\sum_{n \leq x} \log^k \frac{x}{n} = O(x).$$

Beweis.

$$\begin{aligned}\sum_{n \leq x} \log^k \frac{x}{n} &= \sum_{n=2}^{[x]} \log^k \frac{x}{n} + \log^k x \leqq \sum_{n=2}^{[x]} \int_{n-1}^{n} \log^k \frac{x}{t}\, dt + \log^k x \\ &\leqq \int_1^x \log^k \frac{x}{t}\, dt + \log^k x = x \int_1^x \frac{\log^k t}{t^2}\, dt + \log^k x \\ &< x \int_1^\infty \frac{\log^k t}{t^2}\, dt + \log^k x = O(x).\end{aligned}$$

Hilfssatz 5.2.

$$\Lambda(n)\log n+\sum_{t\mid n}\Lambda(t)\,\Lambda\left(\frac{n}{t}\right)=\sum_{t\mid n}\mu(t)\log^2\frac{n}{t}.$$

Beweis. Nach Definition 5.6 der Mangoldtschen Funktion ist

$$\sum_{t\mid n}\Lambda(t)\log t+\sum_{t\mid n}\Lambda(t)\log\frac{n}{t}=\log n\sum_{t\mid n}\Lambda(t)=\log^2 n$$

oder in der Schreibweise der Dirichletschen Multiplikation

$$\Lambda(n)\log n*1+\Lambda(n)*\log n=\log^2 n.$$

Mit $\log n=1*\Lambda(n)$ erhält man

$$\big(\Lambda(n)\log n+\Lambda(n)*\Lambda(n)\big)*1=\log^2 n.$$

Über Satz 5.5 folgt hieraus mit

$$\Lambda(n)\log n+\Lambda(n)*\Lambda(n)=\mu(n)*\log^2 n$$

die Behauptung des Hilfssatzes.

Satz 5.20 (Selbergsche Formel). *Für die Čebyševsche Funktion $\psi(x)$ gilt für $x\to\infty$*

$$\psi(x)\log x+\sum_{n\leqq x}\Lambda(n)\,\psi\left(\frac{x}{n}\right)=2x\log x+O(x).$$

Beweis. Nach Hilfssatz 5.2 ist

$$\sum_{n\leqq x}\Lambda(n)\log n+\sum_{n\leqq x}\sum_{t\mid n}\Lambda(t)\,\Lambda\left(\frac{n}{t}\right)=\sum_{n\leqq x}\sum_{t\mid n}\mu(t)\log^2\frac{n}{t}.$$

Mit Hilfe der Abelschen Identität (4), der Definition 5.12 und Satz 5.14 ergibt sich für die erste Summe

$$\sum_{n\leqq x}\Lambda(n)\log n=\psi(x)\log x-\int_1^x\frac{\psi(t)}{t}\,dt=\psi(x)\log x+O(x).$$

Somit ist

$$\psi(x)\log x+\sum_{n\leqq x}\Lambda(n)\,\psi\left(\frac{x}{n}\right)=A(x)+O(x),$$

wobei

$$A(x)=\sum_{n\leqq x}\sum_{t\mid n}\mu(t)\log^2\frac{n}{t}$$

gesetzt wurde. Es ist also noch $A(x)=2x\log x+O(x)$ zu zeigen. Dazu formen wir

die Summe unter Ausnutzung des soeben erzielten Ergebnisses zunächst etwas um:

$$\begin{aligned} A(x) &= \sum_{n\le x}\sum_{t\mid n}\mu(t)\,(-2\log n\log t+\log^2 t)\\ &= \sum_{n\le x}\left\{2\Lambda(n)\log n+\sum_{t\mid n}\mu(t)\log^2 t\right\}\\ &= \sum_{n\le x}\left\{2\Lambda(n)\log x+\sum_{t\mid n}\mu(t)\log^2 t\right\}+O(x)\\ &= \sum_{n\le x}\sum_{t\mid n}\mu(t)\,(-2\log x\log t+\log^2 t)+O(x)\\ &= \sum_{n\le x}\sum_{t\mid n}\mu(t)\log^2\frac{x}{t}+O(x). \end{aligned}$$

Mit der Eulerschen Konstanten C formen wir weiter um.

$$\begin{aligned} A(x) &= \sum_{n\le x}\sum_{t\mid n}\mu(t)\left(\log^2\frac{x}{t}-C^2\right)+O(x)\\ &= \sum_{t\le x}\mu(t)\left[\frac{x}{t}\right]\left(\log^2\frac{x}{t}-C^2\right)+O(x). \end{aligned}$$

Nach Hilfssatz 5.1 wird daraus

$$A(x) = x\sum_{t\le x}\frac{\mu(t)}{t}\left(\log^2\frac{x}{t}-C^2\right)+O(x)$$

und nach (8)

$$A(x) = x\sum_{t\le x}\frac{\mu(t)}{t}\left(\log\frac{x}{t}-C\right)\left(\sum_{d\le\frac{x}{t}}\frac{1}{d}+O\left(\frac{t}{x}\right)\right)+O(x).$$

Verwendet man wiederum Hilfssatz 5.1, so ergibt sich

$$\begin{aligned} A(x) &= x\sum_{td\le x}\frac{\mu(t)}{td}\left(\log\frac{x}{t}-C\right)+O(x)\\ &= x\sum_{n\le x}\frac{1}{n}\sum_{t\mid n}\mu(t)\left(\log\frac{x}{t}-C\right)+O(x)\\ &= x\log x+x\sum_{n\le x}\frac{\Lambda(n)}{n}+O(x) = 2x\log x+O(x) \end{aligned}$$

nach Satz 5.17. Damit ist die Selbergsche Formel bewiesen.

Aus der Selbergschen Formel soll die *Selbergsche Ungleichung* hergeleitet werden. Wir bereiten dies durch den folgenden Hilfssatz vor.

Hilfssatz 5.3. *Es bezeichne $\psi(x)$ die Čebšyevsche Funktion und $\varrho(x) := \psi(x) - x$. Für $x \to \infty$ gilt*

$$\sum_{n\le x}a_n\left|\varrho\left(\frac{x}{n}\right)\right| = 2\int_1^x\left|\varrho\left(\frac{x}{t}\right)\right|\log t\,dt+O(x\log x)$$

mit

$$a_n = \Lambda(n)\log n + \sum_{t|n} \Lambda(t)\,\Lambda\left(\frac{n}{t}\right).$$

Beweis. Wir verwenden die Abelsche Identität (3) mit $a = 1$, $b = x, f(n) = \left|\varrho\left(\frac{x}{n}\right)\right|$, $g(1) = 0$,

$$g(n) = a_n - 2\int_{n-1}^{n} \log t\,dt \qquad (n \geqq 2).$$

Nach der Selbergschen Formel ist

$$G(x) = \sum_{n\leqq x} a_n - 2\int_1^{[x]} \log t\,dt = O(x).$$

Damit ergibt sich aus (3)

$$\sum_{n\leqq x} a_n \left|\varrho\left(\frac{x}{n}\right)\right| = A_1(x) + A_2(x) + O(x) \tag{17}$$

mit

$$A_1(x) = 2\sum_{2\leqq n\leqq x} \left|\varrho\left(\frac{x}{n}\right)\right| \int_{n-1}^{n} \log t\,dt,$$

$$A_2(x) = \sum_{n\leqq x-1} G(n)\left(\left|\varrho\left(\frac{x}{n}\right)\right| - \left|\varrho\left(\frac{x}{n+1}\right)\right|\right).$$

Wir schätzen nun $A_1(x)$ und $A_2(x)$ einzeln ab. Wir benutzen dabei für $x > y$

$$\big||\varrho(x)| - |\varrho(y)|\big| \leqq |\varrho(x) - \varrho(y)| \leqq \psi(x) - \psi(y) + x - y.$$

Dann ist mit $G(n) = O(n)$ und Satz 5.14

$$\begin{aligned} A_2(x) &= O\left(\sum_{n\leqq x-1} n\left\{\psi\left(\frac{x}{n}\right) + \frac{x}{n} - \psi\left(\frac{x}{n+1}\right) - \frac{x}{n+1}\right\}\right) \\ &= O\left(\sum_{n\leqq x}\left\{\psi\left(\frac{x}{n}\right) + \frac{x}{n}\right\}\right) + O(x) \\ &= O\left(\sum_{n\leqq x}\frac{x}{n}\right) + O(x) = O(x\log x). \end{aligned} \tag{18}$$

Zur Abschätzung von $A_1(x)$ bemerken wir

$$\begin{aligned} &\left|\left|\varrho\left(\frac{x}{n}\right)\right|\int_{n-1}^{n} \log t\,dt - \int_{n-1}^{n}\left|\varrho\left(\frac{x}{t}\right)\right|\log t\,dt\right| \leqq \int_{n-1}^{n}\left|\left|\varrho\left(\frac{x}{n}\right)\right| - \left|\varrho\left(\frac{x}{t}\right)\right|\right|\log t\,dt \\ &\leqq \int_{n-1}^{n}\left\{\psi\left(\frac{x}{t}\right) - \psi\left(\frac{x}{n}\right) + \frac{x}{t} - \frac{x}{n}\right\}\log t\,dt \\ &\leqq (n-1)\left\{\psi\left(\frac{x}{n-1}\right) + \frac{x}{n-1} - \psi\left(\frac{x}{n}\right) - \frac{x}{n}\right\}. \end{aligned}$$

Daher ergibt sich genauso wie bei der Abschätzung von $A_2(x)$

$$A_1(x) = 2\int_1^x \left|\varrho\left(\frac{x}{t}\right)\right| \log t\, dt + O(x \log x). \tag{19}$$

Trägt man (18) und (19) in (17) ein, so erhält man die Behauptung.

Satz 5.21 (Selbergsche Ungleichung). *Es bezeichne $\psi(x)$ die Čebyševsche Funktion und $\varrho(x) = \psi(x) - x$. Für $x \to \infty$ gilt*

$$|\varrho(x)| \log^2 x \leqq 2\int_1^x \left|\varrho\left(\frac{x}{t}\right)\right| \log t\, dt + O(x \log x).$$

Beweis. Wendet man Satz 5.17 auf die Selbergsche Formel an, so erhält man

$$\varrho(x) \log x + \sum_{n \leqq x} \Lambda(n)\, \varrho\left(\frac{x}{n}\right) = O(x).$$

Hieraus ergibt sich weiter

$$\log x \left\{\varrho(x) \log x + \sum_{n \leqq x} \Lambda(n)\, \varrho\left(\frac{x}{n}\right)\right\} - \sum_{m \leqq x} \Lambda(m) \left\{\varrho\left(\frac{x}{m}\right) \log \frac{x}{m} + \sum_{n \leqq \frac{x}{m}} \Lambda(n)\, \varrho\left(\frac{x}{mn}\right)\right\} = O(x \log x) + O\left(x \sum_{m \leqq x} \frac{\Lambda(m)}{m}\right)$$

$$= O(x \log x),$$

$$\varrho(x) \log^2 x = -\sum_{m \leqq x} \Lambda(m)\, \varrho\left(\frac{x}{m}\right) \log m + \sum_{mn \leqq x} \Lambda(m)\, \Lambda(n)\, \varrho\left(\frac{x}{mn}\right) + O(x \log x).$$

Mit der Abkürzung a_n des Hilfssatzes 5.3 folgt

$$|\varrho(x)| \log^2 x \leqq \sum_{n \leqq x} a_n \left|\varrho\left(\frac{x}{n}\right)\right| + O(x \log x),$$

und aus dem Hilfssatz 5.3 selbst ergibt sich die behauptete Selbergsche Ungleichung.

5.4.5. Elementarer Beweis des Primzahlsatzes

Satz 5.22 (Primzahlsatz).

$$\pi(x) \sim \frac{x}{\log x} \qquad (x \to \infty).$$

Nach Satz 5.16 ist der Primzahlsatz äquivalent zu $\psi(x) \sim x$. Dem Beweis dieser Aussage schicken wir noch zwei Hilfssätze voraus.

Hilfssatz 5.4 *Es sei* $\sigma(x) := e^{-x}\varrho(e^x)$, *wobei* $\varrho(y)$ *wie in Hilfssatz* 5.3 *gegeben ist. Dann gibt es eine positive Konstante* A, *so daß für beliebige positive* x_1, x_2

$$\left| \int_{x_1}^{x_2} \sigma(\tau)\, d\tau \right| < A$$

gilt.

Beweis. Nach der Abelschen Identität (4) ist

$$\sum_{n \leq y} \frac{\Lambda(n)}{n} = \frac{\psi(y)}{y} + \int_1^y \frac{\psi(t)}{t^2}\, dt,$$

und hieraus ergibt sich mit Hilfe der Sätze 5.14 und 5.17

$$\int_1^y \left(\frac{\psi(t)}{t^2} - \frac{1}{t} \right) dt = O(1).$$

Mit $t = e^\tau$, $y = e^x$ wird daraus

$$\int_0^x \left(e^{-\tau}\psi(e^\tau) - 1 \right) d\tau = \int_0^x e^{-\tau}\varrho(e^\tau)\, d\tau = \int_0^x \sigma(\tau)\, d\tau = O(1).$$

Folglich ist

$$\int_{x_1}^{x_2} \sigma(\tau)\, d\tau = \int_0^{x_2} \sigma(\tau)\, d\tau - \int_0^{x_1} \sigma(\tau)\, d\tau = O(1).$$

Hilfssatz 5.5. *Ist* $\sigma(x_0) = 0$ *für* $x_0 > 0$, *so ist bei festem* $z > 0$

$$\int_0^z |\sigma(x_0 + \tau)|\, d\tau \leqq \frac{z^2}{2} + O\left(\frac{1}{x_0}\right).$$

Beweis. Wir schreiben die Selbergsche Formel einmal für y und einmal für y_0 auf und bilden die Differenz beider Gleichungen:

$$\psi(y) \log y - \psi(y_0) \log y_0 + \sum_{y_0 < mn \leq y} \Lambda(m)\Lambda(n) = 2(y \log y - y_0 \log y_0) + O(y).$$

Dabei wurde noch $y > y_0 \geqq 1$ vorausgesetzt. Da die Mangoldtsche Funktion nicht negativ ist, erhalten wir hieraus

$$0 \leqq \psi(y) \log y - \psi(y_0) \log y_0 \leqq 2(y \log y - y_0 \log y_0) + O(y),$$

$$|\varrho(y) \log y - \varrho(y_0) \log y_0| \leqq y \log y - y_0 \log y_0 + O(y).$$

Mit $y = e^{x_0+\tau}$, $y_0 = e^{x_0}$, $\sigma(x_0) = 0$ bekommen wir für $0 \leqq \tau \leqq z$

$$|\sigma(x_0+\tau)| \leqq 1 - \frac{x_0}{x_0+\tau}\, e^{-\tau} + O\left(\frac{1}{x_0}\right) = 1 - e^{-\tau} + O\left(\frac{1}{x_0}\right)$$

$$\leqq \tau + O\left(\frac{1}{x_0}\right).$$

Integration über τ von 0 bis z ergibt die Behauptung.

Beweis des Satzes 5.22. In der Selbergschen Ungleichung (Satz 5.21) ersetzen wir x durch e^x, substituieren $t = e^{x-\tau}$ und erhalten

$$x^2\,|\sigma(x)| \leqq 2\int_0^x |\sigma(\tau)|\,(x-\tau)\,d\tau + O(x) = 2\int_0^x\int_0^y |\sigma(\tau)|\,d\tau\,dy + O(x). \qquad (20)$$

Wegen $\psi(x) = O(x)$ ist $\sigma(x)$ beschränkt für $x \to \infty$. Also existieren auch

$$a = \limsup_{x\to\infty} |\sigma(x)|, \qquad b = \limsup_{x\to\infty} \frac{1}{x}\int_0^x |\sigma(\tau)|\,d\tau.$$

Verwendet man in (20) die Folgerung

$$\int_0^x |\sigma(\tau)|\,d\tau \leqq bx + o(x),$$

so erhält man für $|\sigma(x)|$ die Abschätzung

$$|\sigma(x)| \leqq \frac{2}{x^2}\int_0^x \big(by + o(y)\big)\,dy + o(1) = b + o(1).$$

Daher muß $a \leqq b$ sein.

Wegen

$$\sigma(x) = e^{-x}\psi(e^x) - 1$$

ist die Behauptung $\psi(x) \sim x$ äquivalent zu $\sigma(x) \to 0$ für $x \to \infty$. Und dies bedeutet $a = 0$. Wir setzen den Beweis indirekt fort und nehmen $a > 0$ an. Wir werden dann $a > b$ zeigen, was im Widerspruch zu obiger Feststellung steht.

Mit $t > 0$, $\delta = \dfrac{3a^2 + 4A}{2a}$ (A ist die Konstante des Hilfssatzes 5.4) betrachten wir $\sigma(\tau)$ im Intervall $t \leqq \tau \leqq t + \delta - a$. Die Funktion ist dort streng monoton fallend, abgesehen von ihren Unstetigkeiten, in denen sie anwächst. Somit können wir zwei Fälle unterscheiden:

1. Die Funktion $\sigma(\tau)$ besitzt im Intervall wenigstens eine Nullstelle.
2. Die Funktion wechselt im Intervall höchstens einmal das Vorzeichen.

In beiden Fällen wollen wir eine Abschätzung des Integrals

$$\int_t^{t+\delta} |\sigma(\tau)|\, d\tau$$

für große t durchführen.

1. Im betrachteten Intervall gibt es eine Stelle x_0 mit $\sigma(x_0) = 0$. Benutzen wir $|\sigma(t)| \leqq a + o(1)$ und Hilfssatz 5.5 mit $z = a$, so folgt

$$\int_t^{t+\delta} |\sigma(\tau)|\, d\tau = \left\{ \int_t^{x_0} + \int_{x_0}^{x_0+a} + \int_{x_0+a}^{t+\delta} \right\} |\sigma(\tau)|\, d\tau$$

$$\leqq a(x_0 - t) + \frac{a^2}{2} + a(t + \delta - x_0 - a) + o(1) = a'\delta + o(1)$$

mit $a' = a\left(1 - \dfrac{a}{2\delta}\right) < a$.

2. Im betrachteten Intervall wechselt $\sigma(\tau)$ höchstens einmal das Vorzeichen. Liegt im Punkt t_0 mit $t \leqq t_0 \leqq t + \delta - a$ ein Vorzeichenwechsel vor, so ist nach Hilfssatz 5.4

$$\int_t^{t+\delta-a} |\sigma(\tau)|\, d\tau = \left| \int_t^{t_0} \sigma(\tau)\, d\tau \right| + \left| \int_{t_0}^{t+\delta-a} \sigma(\tau)\, d\tau \right| < 2A\,.$$

Liegt gar kein Vorzeichenwechsel vor, so ist

$$\int_t^{t+\delta-a} |\sigma(\tau)|\, d\tau = \left| \int_t^{t+\delta-a} \sigma(\tau)\, d\tau \right| < A\,.$$

Damit ist

$$\int_t^{t+\delta} |\sigma(\tau)|\, d\tau = \left\{ \int_t^{t+\delta-a} + \int_{t+\delta-a}^{t+\delta} \right\} |\sigma(\tau)|\, d\tau$$

$$< 2A + a^2 + o(1) = a'\delta + o(1).$$

Folglich haben wir in beiden Fällen die gleiche Abschätzung

$$\int_t^{t+\delta} |\sigma(\tau)|\, d\tau \leqq a'\delta + o(1),$$

wobei das Restglied für $t \to \infty$ gegen 0 strebt. Ist $X = \left[\dfrac{x}{\delta}\right]$, so erhalten wir

$$\int_0^x |\sigma(\tau)|\, d\tau = \sum_{n=0}^{X-1} \int_{n\delta}^{(n+1)\delta} |\sigma(\tau)|\, d\tau + \int_{X\delta}^{x} |\sigma(\tau)|\, d\tau$$

$$\leqq a' X\delta + o(x) + O(1) = a'x + o(x).$$

Dabei ist

$$b = \limsup_{x\to\infty} \frac{1}{x} \int_0^x |\sigma(\tau)|\, d\tau \leqq a' < a.$$

Dies ist der gewünschte Widerspruch, und der Satz ist bewiesen.

Eine Anwendung des Primzahlsatzes.

Es soll eine asymptotische Darstellung der Summe $\sum p^{-k}$ über alle Primzahlen unterhalb von x für $0 < k < 1$ gegeben werden. Zunächst beweisen wir nur mit Hilfe des in Satz 5.15 gegebenen Čebyševschen Ergebnisses die folgende Abschätzung:

Für $0 < k < 1$ existieren zwei positive Konstanten a, b mit

$$a \frac{x^{1-k}}{\log x} < \sum_{p\leqq x} \frac{1}{p^k} < b \frac{x^{1-k}}{\log x} \qquad (x \geqq 2).$$

Beweis. Den linken Teil der Ungleichung erhalten wir sofort durch

$$\sum_{p\leqq x} \frac{1}{p^k} > x^{-k}\pi(x) > a \frac{x^{1-k}}{\log x}.$$

Für den Nachweis des rechten Teils der Ungleichung schreiben wir

$$\sum_{p\leqq x} \frac{1}{p^k} = \sum_{1<n\leqq x} \frac{1}{n^k} g(n)$$

mit $g(n) = 1$ für $n = p$ und $g(n) = 0$ für $n \neq p$. Die Anwendung von (4) gibt

$$\sum_{p\leqq x} \frac{1}{p^k} = x^{-k}\pi(x) + k \int_1^x t^{-k-1}\pi(t)\, dt < b_1 \frac{x^{1-k}}{\log x} + b_2 \int_2^x \frac{dt}{t^k \log t}.$$

Zur Abschätzung des Integrals sei jetzt δ eine positive Zahl mit $k + \delta < 1$, und t_0 sei so gewählt, daß $t^\delta/\log t$ für $t > t_0 \geqq 2$ monoton wachsend ist. Wir erhalten

$$\sum_{p\leqq x} \frac{1}{p^k} < b_3 \frac{x^{1-k}}{\log x} + b_2 \int_{t_0}^x \left(\frac{t^\delta}{\log t}\right) t^{-k-\delta}\, dt < b_3 \frac{x^{1-k}}{\log x} + b_4 \left(\frac{x^\delta}{\log x}\right) x^{1-k-\delta}$$
$$= b \frac{x^{1-k}}{\log x}.$$

Nun zeigen wir mit Hilfe des Primzahlsatzes die nachstehende Verschärfung:

Satz 5.23. *Für $0 < k < 1$ ist*

$$\sum_{p\leqq x} \frac{1}{p^k} \sim \frac{1}{1-k} \cdot \frac{x^{1-k}}{\log x}.$$

Beweis. Der Primzahlsatz besagt

$$\pi(x) = \frac{x}{\log x} + \varrho(x), \qquad \varrho(x) = o\left(\frac{x}{\log x}\right).$$

In Analogie zum vorstehenden Beweis und zum Beweis des Satzes 5.19 erhalten wir

$$\sum_{p \leqq x} \frac{1}{p^k} = x^{-k}\left(\frac{x}{\log x} + \varrho(x)\right) + k\int_2^x t^{-k-1}\left(\frac{t}{\log t} + \varrho(t)\right) dt$$

$$\sim \frac{x^{1-k}}{\log x} + k\int_2^x \frac{dt}{t^k \log t} \sim \frac{1}{1-k}\cdot\frac{x^{1-k}}{\log x} + \frac{k}{1-k}\int_2^x \frac{dt}{t^k \log^2 t}$$

$$\sim \frac{1}{1-k}\cdot\frac{x^{1-k}}{\log x}.$$

5.5. Die maximale Größenordnung zahlentheoretischer Funktionen

In diesem Abschnitt interessieren wir uns für solche Werte von n, für die die zahlentheoretische Funktion $f(n)$ extrem große Werte annimmt. Dazu müssen wir zunächst einmal eine allgemeine Abschätzung von $f(n)$ haben, und darüber hinaus ist eine präzisere Fragestellung als die angegebene notwendig. Wir werden an Hand der Teilerfunktionen die Aufgabenstellung herausarbeiten und den Begriff der maximalen Größenordnung entwickeln. Anschließend wenden wir ihn auf weitere wichtige Funktionen an.

5.5.1. Die Teilerfunktionen

Es werden die in Definition 5.4 erklärten Teilerfunktionen $\sigma_k(n)$ für $k \geqq 0$ betrachtet. Trivial ist die Abschätzung $\sigma_k(n) \geqq n^k$. Wir bemühen uns um Abschätzungen nach oben und beginnen mit $k > 1$. Bei Benutzung der kanonischen Zerlegung von n erhalten wir

$$\sigma_k(n) = \prod_{i=1}^{r} \frac{{p_i}^{k(\nu_i+1)} - 1}{{p_i}^k - 1} < n^k \prod_{p \mid n}\left(1 - \frac{1}{p^k}\right)^{-1} < n^k \prod_{p}\left(1 - \frac{1}{p^k}\right)^{-1},$$

so daß für alle $n > 1$

$$\sigma_k(n) < \zeta(k)\, n^k$$

gilt. Diese Abschätzung ist außerordentlich gut, denn wir werden zeigen können, daß für unendlich viele Zahlen n die Teilerfunktion dem rechts stehenden Wert beliebig nahe kommt. Dazu betrachten wir die Zahlenfolge $\{n_\nu\}$, $\nu = 2, 3, \ldots$, mit

$$n_\nu = \prod_{p \leqq e^\nu} p^\nu. \tag{21}$$

Beachten wir

$$\prod_{p\leqq e^{\nu}}(1-p^{-k(\nu+1)})>\prod_{p}(1-p^{-k(\nu+1)})=\frac{1}{\zeta\big(k(\nu+1)\big)},$$

so bekommen wir

$$\sigma_k(n_\nu)=n_\nu^{\,k}\prod_{p\leqq e^{\nu}}\frac{1-p^{-k(\nu+1)}}{1-p^{-k}}>\frac{n_\nu^{\,k}}{\zeta\big(k(\nu+1)\big)}\prod_{p\leqq e^{\nu}}(1-p^{-k})^{-1}.$$

Da für $\nu\to\infty$ das verbleibende Produkt konvergent ist und $\zeta\big(k(\nu+1)\big)$ gegen 1 strebt, ist für jedes $\varepsilon>0$ und hinreichend großes ν

$$\sigma_k(n_\nu)>(1-\varepsilon)\,\zeta(k)\,n_\nu^{\,k}.$$

Also haben wir

$$\limsup_{n\to\infty} n^{-k}\sigma_k(n)=\zeta(k)$$

bewiesen. Dies nehmen wir für folgende Definition zum Anlaß.

Definition 5.13. Die zahlentheoretische Funktion $f(n)$ hat die *maximale Größenordnung* $g(n)$, wenn für beliebiges $\varepsilon>0$

$$f(n)<(1+\varepsilon)\,g(n)$$

für alle $n>N(\varepsilon)$ gilt und

$$f(n)>(1-\varepsilon)\,g(n)$$

für unendlich viele Werte von n.

Das über $\sigma_k(n)$ für $k>1$ erzielte Ergebnis läßt sich somit folgendermaßen formulieren:

Satz 5.24 (Gronwall). *Für $k>1$ hat $\sigma_k(n)$ die maximale Größenordnung $\zeta(k)\,n^k$.*

Satz 5.25 (Gronwall). *Die maximale Größenordnung von $\sigma(n)$ ist $e^{C}n\log\log n$. C bedeutet die Eulersche Konstante.*

Beweis. Wie im vorherigen Fall ist

$$\sigma(n)<n\prod_{p\mid n}\left(1-\frac{1}{p}\right)^{-1}.$$

Im Produkt unterscheiden wir die Primteiler p von n mit $p\leqq\log n$ und $p>\log n$. Für die Anzahl s der Primteiler $p>\log n$ gilt $(\log n)^s<n$. Daher ist

$$\begin{aligned}\sigma(n)&<n\prod_{\substack{p\mid n\\ p>\log n}}\left(1-\frac{1}{p}\right)^{-1}\cdot\prod_{\substack{p\mid n\\ p\leqq\log n}}\left(1-\frac{1}{p}\right)^{-1}\\&<n\left(1-\frac{1}{\log n}\right)^{-s}\prod_{p\leqq\log n}\left(1-\frac{1}{p}\right)^{-1}.\end{aligned}$$

Wegen (16) und

$$\left(1-\frac{1}{\log n}\right)^{-s} < \left(1-\frac{1}{\log n}\right)^{-\frac{\log n}{\log\log n}} \sim 1$$

schließen wir auf

$$\sigma(n) < (1+\varepsilon)\, e^{C} n \log\log n$$

für jedes $\varepsilon > 0$ mit $n > N(\varepsilon)$. Damit ist die erste Eigenschaft der maximalen Größenordnung nachgewiesen. Für den zweiten Teil betrachten wir wieder die Folge (21). Nach Satz 5.14 gibt es eine Zahl $B > 0$ mit

$$\log n_\nu = \nu\vartheta(e^\nu) < B\nu e^\nu,$$

$$\log\log n_\nu < \nu + \log(B\nu).$$

Daraus ergibt sich

$$\frac{\sigma(n_\nu)}{e^C n_\nu \log\log n_\nu} = \frac{e^{-C}}{\log\log n_\nu} \prod_{p \leqq e^\nu} \frac{1-p^{-\nu-1}}{1-p^{-1}}$$

$$> \frac{e^{-C}}{\zeta(\nu+1)\,(\nu+\log(B\nu))} \prod_{p \leqq e^\nu} \left(1-\frac{1}{p}\right)^{-1}.$$

Die rechte Seite dieser Ungleichung verhält sich für $\nu \to \infty$ wegen $\zeta(\nu+1) \to 1$ und (16) wie $\dfrac{\nu}{\nu+\log(B\nu)} \sim 1$. Daher ist zu gegebenem $\varepsilon > 0$ für hinreichend großes ν

$$\sigma(n_\nu) > (1-\varepsilon)\, e^C n_\nu \log\log n_\nu,$$

und der Satz ist vollständig bewiesen.

Für $0 \leqq k < 1$ können wir für die Funktionen $\sigma_k(n)$ keine maximalen Größenordnungen angeben, und wir sind gezwungen, zu den Logarithmen überzugehen.

Satz 5.26 (Krätzel). *Für $0 < k < 1$ hat $\log\left(n^{-k}\sigma_k(n)\right)$ die maximale Größenordnung*

$$\frac{1}{1-k} \cdot \frac{(\log n)^{1-k}}{\log\log n}.$$

Für die Funktion $\sigma_k(n)$ selbst heißt das: Es ist mit beliebigem $\varepsilon > 0$

$$\sigma_k(n) < n^k \exp\left\{\frac{1+\varepsilon}{1-k} \cdot \frac{(\log n)^{1-k}}{\log\log n}\right\}$$

für alle $n > N(\varepsilon)$ und

$$\sigma_k(n) > n^k \exp\left\{\frac{1-\varepsilon}{1-k} \cdot \frac{(\log n)^{1-k}}{\log\log n}\right\}$$

für unendlich viele n. Dabei bedeutet $\exp\{z\} := e^z$.

Beweis. Die natürliche Zahl n habe genau r verschiedene Primfaktoren, so daß $n \geqq 2 \cdot 3 \cdot \cdots \cdot p_r$ ist. Sodann ist

$$\log\left(n^{-k}\sigma_k(n)\right) < -\sum_{p|n} \log\left(1-\frac{1}{p^k}\right) \leqq -\sum_{p\leqq p_r} \log\left(1-\frac{1}{p^k}\right),$$

$$\log\left(n^{-k}\sigma_k(n)\right) < S_1 + S_2 \tag{22}$$

mit

$$S_1 = -\sum_{p\leqq \log n} \log\left(1-\frac{1}{p^k}\right),$$

$$S_2 = 0 \quad \text{für} \quad p_r \leqq \log n, \qquad S_2 = -\sum_{\log n < p \leqq p_r} \log\left(1-\frac{1}{p^k}\right) \text{ für } p_r > \log n.$$

Für S_1 erhalten wir bei Benutzung von Satz 5.23

$$S_1 = \sum_{p\leqq \log n} \frac{1}{p^k}\left\{1 + O\left(\frac{1}{p^k}\right)\right\} = \frac{1}{1-k}\cdot\frac{(\log n)^{1-k}}{\log\log n}\{1+o(1)\},$$

$$S_1 < \frac{1+\varepsilon/2}{1-k}\cdot\frac{(\log n)^{1-k}}{\log\log n} \tag{23}$$

für jedes $\varepsilon > 0$ und hinreichend großes n.

Ist $S_2 = 0$, so sind wir bereits fertig. Nehmen wir also $p_r > \log n$ an. Damit wächst mit n auch p_r. Nachfolgend seien die ε_i stets beliebig positiv, und die Abschätzungen sind gültig für $n > N(\varepsilon_i)$. Aus $\log n \geqq \vartheta(p_r)$, dem Primzahlsatz und Satz 5.16 folgt $p_r < (1+\varepsilon_1)\log n$. Daher ist

$$\begin{aligned} S_2 &< -\log\left(1-\frac{1}{\log^k n}\right)\{\pi(p_r) - \pi(\log n)\} \\ &< -\log\left(1-\frac{1}{\log^k n}\right)\left\{\frac{(1+\varepsilon_2)\,p_r}{\log p_r} - \frac{(1-\varepsilon_3)\log n}{\log\log n}\right\} \\ &< -\varepsilon_4\frac{\log n}{\log\log n}\log\left(1-\frac{1}{\log^k n}\right) < -\varepsilon_5\pi(\log n)\log\left(1-\frac{1}{\log^k n}\right) \\ &< -\varepsilon_5\sum_{p\leqq\log n}\log\left(1-\frac{1}{p^k}\right) = \varepsilon_5 S_1. \end{aligned}$$

Verwenden wir die Abschätzung (23), so erzielen wir für jedes $\varepsilon > 0$ und hinreichend großes n

$$S_2 < \frac{\varepsilon/2}{1-k}\cdot\frac{(\log n)^{1-k}}{\log\log n}.$$

Setzen wir dies und (23) in (22) ein, so erhalten wir den ersten Teil der Behauptung.

Für den Nachweis der zweiten Eigenschaft der maximalen Größenordnung wählen wir uns die Zahlenfolge $\{n_\nu\}$, $\nu = 1, 2, \ldots$, mit $n_\nu = 2 \cdot 3 \cdot \cdots \cdot p_\nu$ aus. Für die Folge ist mit $\varepsilon_1 > 0$, hinreichend großem ν nach Satz 5.23

$$\log\left(n_\nu^{-k}\sigma_k(n_\nu)\right) = \sum_{p \leqq p_\nu} \log \frac{1 - p^{-2k}}{1 - p^{-k}} = \sum_{p \leqq p_\nu} \log\left(1 + \frac{1}{p^k}\right) > \frac{1 - \varepsilon_1}{1 - k} \cdot \frac{p_\nu^{1-k}}{\log p_\nu}.$$

Benutzen wir mit dem Primzahlsatz wieder $\log n_\nu = \vartheta(p_\nu) \sim p_\nu$, so ist für alle $\varepsilon > 0$

$$\log\left(n_\nu^{-k}\sigma_k(n_\nu)\right) > \frac{1 - \varepsilon}{1 - k} \cdot \frac{(\log n_\nu)^{1-k}}{\log\log n_\nu},$$

sofern ν genügend groß ist. Dieses vollendet den Beweis.

Bei der Bestimmung der maximalen Größenordnung von $\log d(n)$ wird wesentlich die Tatsache ausgenutzt, daß $d(p^\nu) = \nu + 1$ unabhängig von der Primzahl p ist. Da uns außer an dieser Stelle noch in 5.5.3. und 7.3. solche „primzahlunabhängigen" Funktionen begegnen werden, soll hier gleich ein allgemeineres Resultat erzielt werden.

Satz 5.27 (Drozdova/Freiman). *Es sei $f(n)$ eine multiplikative, primzahlunabhängige Funktion, d. h., es ist $f(p^\nu) = g(\nu)$ unabhängig von der Primzahl p. Dabei sei $g(\nu) \geqq 1$, und es existiere ein ν_0 mit $g(\nu_0) > 1$. Für große ν sei $g(\nu)$ durch $\log g(\nu) = O(\nu^{1-a})$ mit $a > 0$ eingeschränkt. Dann ist die maximale Größenordnung von $\log f(n)$ gegeben durch*

$$\frac{\log g(k)}{k} \cdot \frac{\log n}{\log\log n}.$$

Dabei ist k die durch

$$\frac{\log g(\nu)}{\nu} \begin{cases} \leqq \dfrac{\log g(k)}{k} & \text{für} \quad \nu \leqq k, \\ < \dfrac{\log g(k)}{k} & \text{für} \quad \nu > k \end{cases}$$

eindeutig bestimmte natürliche Zahl.

Für die Funktion $f(n)$ selbst besagt der Satz, daß

$$f(n) < \left(g(k)\right)^{\frac{1+\varepsilon}{k} \cdot \frac{\log n}{\log\log n}}$$

für $n > N(\varepsilon)$ ist und

$$f(n) > \left(g(k)\right)^{\frac{1-\varepsilon}{k} \cdot \frac{\log n}{\log\log n}}$$

für unendlich viele n.

Beweis. Wir können $0 < a \leqq 1$ annehmen. Mit $\delta > 0$ und der kanonischen Zerlegung von n bilden wir

$$\frac{f(n)}{n^\delta} = \prod_{i=1}^{r} \frac{g(\nu_i)}{p_i^{\nu_i\delta}}.$$

Nach Voraussetzung ist mit einer geeigneten Konstanten $b > 0$

$$\frac{g(\nu)}{p^{\nu\delta}} < e^{b\nu^{1-a} - \nu\delta\log 2}.$$

Die Funktion

$$h(\delta) = c\delta^{1-\frac{1}{a}} + \nu\delta\log 2 \qquad (c > 0)$$

nimmt für $0 < a < 1$ ihr Minimum an der Stelle

$$\delta_0 = \left(\frac{c(1/a - 1)}{\nu \log 2}\right)^a$$

an. Daher ist

$$h(\delta) \geqq b\nu^{1-a},$$

falls man noch c entsprechend wählt. Folglich ist für $0 < a < 1$

$$\frac{g(\nu)}{p^{\nu\delta}} < e^{c\delta^{1-1/a}}.$$

Eine solche Ungleichung besteht aber offensichtlich auch für $a = 1$. Für $p^{k\delta} \geqq g(k)$ ist

$$\frac{g(\nu)}{p^{\nu\delta}} \leqq \frac{g(\nu)}{\left(g(k)\right)^{\nu/k}} \leqq 1$$

nach Voraussetzung. Daher folgt

$$\log f(n) \leqq \delta \log n + \sum_{p^{k\delta} \leqq g(k)} c\delta^{1-\frac{1}{a}} \leqq \delta \log n + c\delta^{1-\frac{1}{a}} \left(g(k)\right)^{\frac{1}{k\delta}}.$$

Mit

$$\delta = \frac{(1 + \varepsilon/2)\log g(k)}{k \log\log n}$$

wird

$$\log f(n) \leqq \left(1 + \frac{\varepsilon}{2}\right) \frac{\log g(k)}{k} \cdot \frac{\log n}{\log\log n} + \frac{c(\log n)^{\frac{1}{1+\varepsilon/2}}}{k^{1-1/a}} \left(\frac{(1 + \varepsilon/2)\log g(k)}{\log\log n}\right)^{1-\frac{1}{a}}$$

$$\leqq (1 + \varepsilon) \frac{\log g(k)}{k} \cdot \frac{\log n}{\log\log n}$$

für $n > N(\varepsilon)$. Dies ist der erste Teil der Behauptung.

Nun betrachten wir die Zahlenfolge $\{n_\nu\}$, $\nu = 1, 2, \ldots$, mit $n_\nu = (2 \cdot 3 \cdot \cdots \cdot p_\nu)^k$. Für diese Zahlen ist

$$f(n_\nu) = \big(g(k)\big)^{\pi(p_\nu)}.$$

Nach Satz 5.14 gibt es eine positive Konstante A mit

$$Ap_\nu < \vartheta(p_\nu) = \frac{1}{k} \log n_\nu \leqq \pi(p_\nu) \log p_\nu.$$

Daraus folgt

$$\log f(n_\nu) = \pi(p_\nu) \log g(k) \geqq \frac{\log g(k)}{k} \cdot \frac{\log n_\nu}{\log p_\nu} > \frac{\log g(k)}{k} \cdot \frac{\log n_\nu}{\log \log n_\nu - \log (Ak)}$$

$$> (1 - \varepsilon) \frac{\log g(k)}{k} \cdot \frac{\log n_\nu}{\log \log n_\nu}$$

für $n_\nu > N(\varepsilon)$. Dies war zu beweisen.

Satz 5.28 (Wigert). *Die maximale Größenordnung von* $\log d(n)$ *ist*

$$\log 2 \frac{\log n}{\log \log n}.$$

Beweis. In den Bezeichnungen des Satzes 5.27 ist $f(n) = d(n)$, $f(p^\nu) = g(\nu) = \nu + 1$. Die Größe a kann beliebig in $0 < a < 1$ angenommen werden. Schließlich ist $k = 1$. Aus $g(1) = 2$ folgt dann sofort die Behauptung.

5.5.2. Die Eulersche φ-Funktion

Die Bestimmung der maximalen Größenordnung der Eulerschen φ-Funktion ist recht einfach. Trivialerweise ist für alle n stets $\varphi(n) \leqq n$. Für die Folge $\{n_\nu\}$, $\nu = 1, 2, \ldots$, mit $n_\nu = p_\nu$ ist

$$\varphi(n_\nu) = n_\nu \left(1 - \frac{1}{p_\nu}\right).$$

Wählt man zu $\varepsilon > 0$ die Primzahlen $p_\nu > 1/\varepsilon$, so ist $\varphi(n_\nu) > n_\nu(1 - \varepsilon)$. Damit ist bewiesen:

Satz 5.29. *Die maximale Größenordnung von* $\varphi(n)$ *ist* n.

Satz 5.30. *Für* $n > 1$ *ist*

$$\frac{1}{\zeta(2)} < \frac{\sigma(n)\, \varphi(n)}{n^2} < 1.$$

Ohne Beweis sei $\zeta(2) = \pi^2/6$ angemerkt.

Beweis. Aus der kanonischen Zerlegung von n ergibt sich

$$\frac{\sigma(n)\,\varphi(n)}{n^2} = \prod_{i=1}^{r}(1 - p_i^{-\nu_i-1}),$$

und für das Produkt ist

$$\frac{1}{\zeta(2)} = \prod_{p}(1 - p^{-2}) < \prod_{i=1}^{r}(1 - p_i^{-\nu_i-1}) < 1.$$

Nach diesem Satz hat die Funktion $\frac{n}{\varphi(n)}$ die gleiche Größenordnung wie $\frac{\sigma(n)}{n}$. Wir zeigen, daß sogar die maximalen Größenordnungen übereinstimmen.

Satz 5.31 (Landau). *Die maximale Größenordnung von* $\frac{n}{\varphi(n)}$ *ist* $e^C \log\log n$, *wobei* C *die Eulersche Konstante bedeutet.*

Beweis. Aus

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

folgern wir entsprechend der Teilerfunktion $\sigma(n)$

$$\frac{n}{\varphi(n)} < \left(1 - \frac{1}{\log n}\right)^{-\frac{\log n}{\log\log n}} \prod_{p \leqq \log n}\left(1 - \frac{1}{p}\right)^{-1}$$

und mit $\varepsilon > 0$

$$\frac{n}{\varphi(n)} < (1 + \varepsilon)\, e^C \log\log n$$

für $n > N(\varepsilon)$. Die Existenz unendlich vieler Zahlen n mit

$$\frac{n}{\varphi(n)} > (1 - \varepsilon)\, e^C \log\log n$$

folgt aus

$$\frac{n}{\varphi(n)} > \frac{\sigma(n)}{n}$$

und Satz 5.25.

5.5.3. Die Anzahl der Primfaktoren natürlicher Zahlen

Die Funktionen $\omega(n)$ (Anzahl der verschiedenen Primfaktoren von n) und $\Omega(n)$ (Anzahl aller Primfaktoren von n) zeigen ein sehr irreguläres Verhalten. Einerseits ist für eine Primzahl $n = p$ immer $\omega(p) = \Omega(p) = 1$, andererseits können diese Funk-

tionen auch recht große Werte annehmen. Aus der kanonischen Zerlegung von n folgt sofort

$$n \geqq 2^{\Omega(n)}$$

und

$$\Omega(n) \leqq \frac{\log n}{\log 2}.$$

Dabei gilt für die Zahlenfolge $\{n_\nu\}$ mit $n_\nu = 2^\nu$, $\nu = 1, 2, \ldots$, stets

$$\Omega(n_\nu) = \nu = \frac{\log n_\nu}{\log 2}.$$

Mithin haben wir:

Satz 5.32. *Die maximale Größenordnung von $\Omega(n)$ ist* $\dfrac{\log n}{\log 2}$.

Satz 5.33. *Die maximale Größenordnung von $\omega(n)$ ist* $\dfrac{\log n}{\log \log n}$.

Beweis. Die Funktion $f(n) = 2^{\omega(n)}$ ist multiplikativ und primzahlunabhängig. In Satz 5.27 setzen wir $f(p^\nu) = g(\nu) = 2$, $a = 1$, $k = 1$. Daraus folgt sogleich die Behauptung.

5.6. Ramanujansche Reihen

Von S. Ramanujan (1887—1920) wurde eine Möglichkeit der Entwicklung zahlentheoretischer Funktionen in unendliche Reihen aufgedeckt, die einen gewissen Aufschluß über die Größenverhältnisse erlaubt. Es soll dies hier für die Teilerfunktionen und die Eulersche φ-Funktion demonstriert werden. Grundlage bilden die in Abschnitt 3.4 erwähnten *Ramanujanschen Summen*

$$c_m(a) = \sum_{\substack{n=1 \\ (n,m)=1}}^{m} e^{\frac{2\pi i a n}{m}}. \tag{24}$$

Sie sind nach Satz 3.7 hinsichtlich m multiplikative Funktionen. Demzufolge ist auch die Funktion

$$\eta_m(a) = \sum_{t \mid m} c_t(a) \tag{25}$$

bezüglich m multiplikativ. Wir wollen sie berechnen, wobei wir uns also auf Primzahlpotenzen $m = p^\nu$ beschränken können. Ist $p^\nu \mid a$, so ist nach Satz 3.7

$$\eta_{p^\nu}(a) = 1 + \sum_{r=1}^{\nu} c_{p^r}(a) = 1 + \sum_{r=1}^{\nu} p^{r-1}(p-1) = p^\nu.$$

Ist $p^r \nmid a$, so gibt es ein k mit $0 \leqq k < r$ und $p^k \mid a$ und $p^{k+1} \nmid a$, und nach Satz 3.7 folgt

$$\eta_{p^r}(a) = 1 + \sum_{r=1}^{k} p^{r-1}(p-1) - p^k = 0.$$

Auf Grund der Multiplikativität ist insgesamt $\eta_m(a) = m$ für $m \mid a$ und $\eta_m(a) = 0$ für $m \nmid a$. Wenden wir auf (25) die Möbiussche Umkehrformel an, so erhalten wir

$$c_m(a) = \sum_{t \mid m} \mu\left(\frac{m}{t}\right) \eta_t(a),$$

$$c_m(a) = \sum_{t \mid a, t \mid m} t\mu\left(\frac{m}{t}\right). \tag{26}$$

Als ein interessantes Nebenergebnis erhalten wir aus (26) $c_m(1) = \mu(m)$ und nach (24)

$$\mu(m) = \sum_{\substack{n=1 \\ (n,m)=1}}^{m} e^{2\pi i \frac{n}{m}}.$$

Nun betrachten wir eine Entwicklung von $\sigma_k(n)$ für $k > 0$.

$$\frac{1}{\zeta(k+1)} \frac{\sigma_k(n)}{n^k} = \frac{1}{\zeta(k+1)} \sum_{d \mid n} \left(\frac{d}{n}\right)^k = \frac{1}{\zeta(k+1)} \sum_{t \mid n} \frac{1}{t^k}$$

$$= \sum_{d=1}^{\infty} \frac{\mu(d)}{d^{k+1}} \sum_{t \mid n} \frac{t}{t^{k+1}} = \sum_{m=1}^{\infty} \frac{1}{m^{k+1}} \sum_{t \mid n, dt = m} t\mu(d)$$

$$= \sum_{m=1}^{\infty} \frac{1}{m^{k+1}} \sum_{t \mid n, t \mid m} t\mu\left(\frac{m}{t}\right).$$

Bei Verwendung von (26) und der Bemerkung $|c_m(n)| \leqq \sigma(n)$, woraus die Konvergenz der Reihe für $k > 0$ folgt, erhalten wir:

Satz 5.34. *Für $k > 0$ ist*

$$\sigma_k(n) = \zeta(k+1)\, n^k \sum_{m=1}^{\infty} \frac{c_m(n)}{m^{k+1}}.$$

Errechnet man aus (24) die ersten Werte von $c_m(n)$, so erkennt man aus

$$\sigma_k(n) = \zeta(k+1)\, n^k \left\{1 + \frac{(-1)^n}{2^{k+1}} + \frac{2\cos\frac{2\pi n}{3}}{3^{k+1}} + \frac{2\cos\frac{\pi n}{2}}{4^{k+1}} + \cdots\right\}$$

das Schwanken von $\sigma_k(n)$ um einen „Mittelwert" $\zeta(k+1)\, n^k$.
Darauf werden wir im nächsten Abschnitt bezug nehmen.

Eine entsprechende Darstellung wollen wir jetzt für die *Eulersche φ-Funktion* herleiten. Damit das Wesen der Entwicklung deutlicher in Erscheinung tritt, werde noch eine Verallgemeinerung dieser Funktion vorgenommen.

Definition 5.14. Für $k = 1, 2, \ldots$ werde die *Jordansche Funktion* $J_k(n)$ durch

$$J_k(n) = n^k \prod_{p|n} \left(1 - \frac{1}{p^k}\right)$$

erklärt.

Speziell ist $J_1(n) = \varphi(n)$. Auf Grund der Definition ist $J_k(n)$ natürlich multiplikativ. Wegen

$$\sum_{t|p^\nu} J_k(t) = 1 + \sum_{r=1}^{\nu} p^{(r-1)k}\,(p^k - 1) = p^{\nu k}$$

ist

$$\sum_{t|n} J_k(t) = n^k$$

und mittels der Möbiusschen Umkehrformel

$$J_k(n) = \sum_{t|n} \left(\frac{n}{t}\right)^k \mu(t).$$

Betrachten wir jetzt entsprechend den Teilerfunktionen die Entwicklung von $J_k(n)$.

$$\frac{J_k(n)}{n^k} = \sum_{t|n} \frac{\mu(t)}{t^k} = \sum_{t=1}^{\infty} \frac{\mu(t)}{t^{k+1}} \sum_{m|t} c_m(n)$$

$$= \sum_{m=1}^{\infty} \frac{c_m(n)}{m^{k+1}} \sum_{d=1}^{\infty} \frac{\mu(dm)}{d^{k+1}} = \sum_{m=1}^{\infty} \frac{c_m(n)\,\mu(m)}{m^{k+1}} \sum_{\substack{d=1 \\ (d,m)=1}}^{\infty}{}' \frac{\mu(d)}{d^{k+1}}.$$

Nun wenden wir den Satz 5.7 auf die multiplikative Funktion

$$f(d) = \begin{cases} \mu(d) & \text{für } (d, m) = 1, \\ 0 & \text{für } (d, m) > 1 \end{cases}$$

an und erhalten

$$\sum_{\substack{d=1 \\ (d,m)=1}}^{\infty}{}' \frac{\mu(d)}{d^{k+1}} = \sum_{d=1}^{\infty} \frac{f(d)}{d^{k+1}} = \prod_{p} \left(\sum_{\nu=0}^{\infty} \frac{f(p^\nu)}{p^{\nu(k+1)}}\right) = \prod_{p \nmid m} \left(1 - \frac{1}{p^{k+1}}\right)$$

$$= \frac{1}{\zeta(k+1)} \prod_{p|m} \left(1 - \frac{1}{p^{k+1}}\right)^{-1},$$

also

$$\frac{J_k(n)}{n^k} = \sum_{m=1}^{\infty} \frac{c_m(n)\,\mu(m)}{m^{k+1}\,\zeta(k+1)} \prod_{p|m} \left(1 - \frac{1}{p^{k+1}}\right)^{-1}.$$

Daraus ergibt sich:

Satz 5.35. *Für* $k = 1, 2, \ldots$ *ist*

$$J_k(n) = \frac{n^k}{\zeta(k+1)} \sum_{m=1}^{\infty} \frac{c_m(n)\,\mu(m)}{J_{k+1}(m)}.$$

Insbesondere ist für $k = 1$ *mit* $\zeta(2) = \dfrac{\pi^2}{6}$

$$\varphi(n) = \frac{6n}{\pi^2} \sum_{m=1}^{\infty} \frac{c_m(n)\ \mu(m)}{J_2(m)}.$$

Aus

$$\varphi(n) = \frac{6n}{\pi^2}\left\{1 - \frac{(-1)^n}{2^2-1} - \frac{2\cos\dfrac{2\pi n}{3}}{3^2-1} \pm \cdots\right\}$$

erkennt man wieder ein Schwanken von $\varphi(n)$ um den „Mittelwert" $\dfrac{6n}{\pi^2}$.

5.7. Die durchschnittliche Größenordnung zahlentheoretischer Funktionen

Die Betrachtungen des vorigen Abschnittes veranlassen uns zu folgender Definition.

Definition 5.15. Die zahlentheoretische Funktion $f(n)$ heißt von der *durchschnittlichen Größenordnung* der zahlentheoretischen Funktion $g(n)$, wenn

$$\sum_{n \leqq x} f(n) \sim \sum_{n \leqq x} g(n)$$

für $x \to \infty$ ist.

Um eine Vorstellung über eine zahlentheoretische Funktion $f(n)$ zu erhalten, streben wir natürlich die Angabe einer möglichst einfachen Funktion $g(n)$ an. Wir werden dann auch sagen: $f(n)$ *hat die durchschnittliche Größenordnung* $g(n)$.

Es sollen spezielle zahlentheoretische Funktionen auf ihre durchschnittliche Größenordnung hin untersucht werden.

5.7.1. Die Eulersche φ-Funktion

Satz 5.36 (Mertens). *Die durchschnittliche Größenordnung von* $\varphi(n)$ *ist* $\dfrac{6}{\pi^2}\, n$. *Genauer gilt*

$$\sum_{n \leqq x} \varphi(n) = \frac{3}{\pi^2} x^2 + O(x \log x).$$

Beweis. Aus $\varphi(n) = n * \mu(n)$ ergibt sich

$$\varphi(n) = \sum_{td=n} d\mu(t)$$

und

$$\sum_{n\leqq x}\varphi(n)=\sum_{td\leqq x}d\mu(t)=\sum_{t\leqq x}\mu(t)\sum_{d\leqq x/t}d=\frac{1}{2}\sum_{t\leqq x}\mu(t)\left\{\left[\frac{x}{t}\right]^2+\left[\frac{x}{t}\right]\right\}$$

$$=\frac{1}{2}\sum_{t\leqq x}\mu(t)\left\{\left(\frac{x}{t}\right)^2+O\left(\frac{x}{t}\right)\right\}=\frac{x^2}{2}\sum_{t\leqq x}\frac{\mu(t)}{t^2}+O(x\log x).$$

Es ist

$$\sum_{t\leqq x}\frac{\mu(t)}{t^2}=\sum_{t=1}^{\infty}\frac{\mu(t)}{t^2}+O\left(\sum_{t>x}\frac{1}{t^2}\right)=\frac{1}{\zeta(2)}+O\left(\frac{1}{x}\right)$$

und daher

$$\sum_{n\leqq x}\varphi(n)=\frac{x^2}{2\zeta(2)}+O(x\log x).$$

Mit $\zeta(2)=\dfrac{\pi^2}{6}$ folgt die Behauptung.

5.7.2. Quadratsummen

Definition 5.16. Es bezeichnet $r(n)$ die *Anzahl der Darstellungen der natürlichen Zahl n als Summe von zwei Quadraten* ganzer Zahlen. *Es sei* $r(0)=1$.

Man kann

$$r(n)=\sum_{n_1^2+n_2^2=n}1$$

schreiben, wobei n_1, n_2 alle diejenigen ganzen Zahlen durchlaufen, die der Gleichung $n_1^2+n_2^2=n$ genügen. Einige Beispiele: $r(1)=4$, $r(2)=4$, $r(3)=0$, $r(4)=4$, $r(5)=8$. Da stets $n_1^2+n_2^2\not\equiv 3 \pmod 4$ ist, haben wir $r(n)=0$ für $n\equiv 3 \pmod 4$. Man kann $r(n)$ für beliebiges n berechnen. Das muß aber bis zum Abschnitt 6.2 verschoben werden. Wir bestimmen hier die durchschnittliche Größenordnung.

Satz 5.37 (Gauss). *Die durchschnittliche Größenordnung von* $r(n)$ *ist* π. *Genauer gilt*

$$R(x)=\sum_{0\leqq n\leqq x}r(n)=\pi x+O\left(\sqrt{x}\right).$$

Beweis. Setzt man in $R(x)$ die Summendarstellung von $r(n)$ ein, so ist

$$R(x)=4\sum_{\substack{n_1^2+n_2^2\leqq x\\ n_1,n_2\geqq 0}}{}''1.$$

Dabei wurde die Summation durch Ausnutzung von Symmetrieeigenschaften auf nichtnegative Zahlen n_1, n_2 beschränkt. Ein Strich am Summenzeichen bedeutet, daß der Summand für $n_1=0$ den Faktor $\dfrac{1}{2}$ erhält. Der zweite Strich bezieht sich

analog auf $n_2 = 0$. Wir erhalten weiter

$$R(x) = 4 \sum_{0 \le n_1 \le \sqrt{x}}' \sum_{0 \le n_2 \le \sqrt{x - n_1^2}}' 1 = 4 \sum_{0 \le n \le \sqrt{x}}' \left\{ \left[\sqrt{x - n^2} \right] + \frac{1}{2} \right\}$$
$$= 4 \sum_{0 \le n \le \sqrt{x}} \sqrt{x - n^2} + O\left(\sqrt{x}\right).$$

Mit der Euler-Maclaurinschen Summenformel und $\psi(t) = t - [t] - \frac{1}{2}$ ist

$$R(x) = 4 \int_0^{\sqrt{x}} \sqrt{x - t^2}\, dt - 4 \int_0^{\sqrt{x}} \frac{t}{\sqrt{x - t^2}}\, \psi(t)\, dt + O\left(\sqrt{x}\right)$$
$$= 4x \int_0^1 \sqrt{1 - t^2}\, dt - 4\sqrt{x} \int_0^1 \frac{t}{\sqrt{1 - t^2}}\, \psi\left(\sqrt{x}\, t\right) dt + O\left(\sqrt{x}\right).$$

Das erste Integral ist der vierte Teil des Flächeninhalts des Einheitskreises, und das zweite Integral ist beschränkt. Damit ergibt sich die Behauptung.

5.7.3. Die Teilerfunktionen

Satz 5.38. *Die durchschnittliche Größenordnung von $\sigma_k(n)$ ist $\zeta(k+1)\, n^k$ für $k > 0$. Genauer gilt*

$$\sum_{n \le x} \sigma_k(n) = \frac{\zeta(k+1)}{k+1}\, x^{k+1} + \begin{cases} O(x^k) & \text{für } k > 1, \\ O(x \log x) & \text{für } k = 1, \\ O(x) & \text{für } 0 < k < 1. \end{cases}$$

Beweis.

$$\sum_{n \le x} \sigma_k(n) = \sum_{n \le x} \sum_{t \mid n} t^k = \sum_{td \le x} t^k = \sum_{d \le x} \sum_{t \le x/d} t^k$$
$$= \sum_{d \le x} \left\{ \frac{1}{k+1} \left(\frac{x}{d}\right)^{k+1} + O\left(\left(\frac{x}{d}\right)^k\right) \right\}.$$

Für $k > 0$ ist

$$\sum_{d \le x} \frac{1}{d^{k+1}} = \zeta(k+1) + O\left(\frac{1}{x^k}\right)$$

und

$$\sum_{d \le x} \frac{1}{d^k} = \begin{cases} O(1) & \text{für } k < 1, \\ O(\log x) & \text{für } k = 1, \\ O(x^{1-k}) & \text{für } 0 < k < 1. \end{cases}$$

Satz 5.39 (Dirichlet). *Die durchschnittliche Größenordnung von $d(n)$ ist* $\log n$. *Genauer gilt mit der Eulerschen Konstanten C*

$$D(x) = \sum_{n \leq x} d(n) = x \log x + (2C - 1)\, x + O\left(\sqrt{x}\right).$$

Beweis. Der Nachweis der durchschnittlichen Größenordnung $\log n$ von $d(n)$ ist ganz einfach:

$$D(x) = \sum_{td \leq x} 1 = \sum_{d \leq x} \left[\frac{x}{d}\right] = \sum_{d \leq x} \left\{\frac{x}{d} + O(1)\right\} = x \log x + O(x).$$

Das präzisere Ergebnis erhält man folgendermaßen durch Ausnutzung von Symmetrieeigenschaften:

$$\begin{aligned} D(x) &= \sum_{d \leq \sqrt{x}} \sum_{t \leq x/d} 1 + \sum_{\substack{td \leq x \\ \sqrt{x} < d \leq x}} 1 = \sum_{d \leq \sqrt{x}} \sum_{t \leq x/d} 1 + \sum_{t < \sqrt{x}} \sum_{\sqrt{x} < d \leq x/t} 1 \\ &= 2 \sum_{d \leq \sqrt{x}} \sum_{t \leq x/d} 1 - \left[\sqrt{x}\right]^2 = 2 \sum_{d \leq \sqrt{x}} \left\{\frac{x}{d} + O(1)\right\} - x + O\left(\sqrt{x}\right) \\ &= 2x \log \sqrt{x} + (2C - 1)\, x + O\left(\sqrt{x}\right). \end{aligned}$$

Es werden noch allgemeinere Teilerfunktionen betrachtet.

Definition 5.17. Für natürliche Zahlen a, b bezeichne

$$d(a, b; n) := \sum_{t_1^a t_2^b = n} 1.$$

Satz 5.40. *Für* $1 \leq a < b$ gilt

$$D(a, b; x) = \sum_{n \leq x} d(a, b; n) = \zeta\left(\frac{b}{a}\right) x^{1/a} + \zeta\left(\frac{a}{b}\right) x^{1/b} + O\left(x^{\frac{1}{a+b}}\right).$$

Beweis.

$$\begin{aligned} D(a, b; x) &= \sum_{t_1^a t_2^b \leq x} 1 = \sum_{t_1^{a+b} \leq x} \sum_{t_2^b \leq x t_1^{-a}} 1 + \sum_{t_2^{a+b} \leq x} \sum_{x^{1/(a+b)} < t_1 \leq (x t_2^{-b})^{1/a}} 1 \\ &= \sum_{t^{a+b} \leq x} \left\{\left[\left(\frac{x}{t^b}\right)^{1/a}\right] + \left[\left(\frac{x}{t^a}\right)^{1/b}\right]\right\} - \left[x^{\frac{1}{a+b}}\right]^2 \\ &= \sum_{t^{a+b} \leq x} \left\{\left(\frac{x}{t^b}\right)^{1/a} + \left(\frac{x}{t^a}\right)^{1/b}\right\} - x^{\frac{2}{a+b}} + O\left(x^{\frac{1}{a+b}}\right) \\ &= \zeta\left(\frac{b}{a}\right) x^{1/a} + \zeta\left(\frac{a}{b}\right) x^{1/b} + O\left(x^{\frac{1}{a+b}}\right) \end{aligned}$$

unter Verwendung von (10).

5.7.4. Quadratfreie Zahlen

Satz 5.41. *Die Anzahl der quadratfreien Zahlen unterhalb x ist*

$$\sum_{n\leqq x} |\mu(n)| = \frac{6}{\pi^2}\, x + O\big(\sqrt{x}\big).$$

Beweis. Aus

$$\sum_{n=1}^{\infty} \frac{|\mu(n)|}{n^s} = \frac{\zeta(s)}{\zeta(2s)} = \sum_{d=1}^{\infty} \frac{1}{d^s} \sum_{t=1}^{\infty} \frac{\mu(t)}{t^{2s}}$$

folgt unter Beachtung von Satz 5.6

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

und

$$\sum_{n\leqq x} |\mu(n)| = \sum_{t^2 d\leqq x} \mu(t) = \sum_{t^2\leqq x} \mu(t) \sum_{d\leqq x/t^2} 1$$

$$= \sum_{t^2\leqq x} \mu(t) \left[\frac{x}{t^2}\right] = x \sum_{t^2\leqq x} \frac{\mu(t)}{t^2} + O\big(\sqrt{x}\big) = \frac{x}{\zeta(2)} + O\big(\sqrt{x}\big).$$

5.7.5. Die Anzahl der Primfaktoren natürlicher Zahlen

In 5.5.3 wurde auf das irreguläre Verhalten der Funktionen $\omega(n)$, $\Omega(n)$ hingewiesen. Es ist zwar für quadratfreie Zahlen n stets $\omega(n) = \Omega(n)$, sonst immer $\Omega(n) > \omega(n)$, und auch die maximale Größenordnung von $\Omega(n)$ ist größer als die von $\omega(n)$, dennoch haben beide Funktionen die gleiche durchschnittliche Größenordnung und sogar noch weitere Eigenschaften wie sich in diesem Abschnitt und in 5.8 zeigen wird.

Satz 5.42 (Hardy/Ramanujan). *Die durchschnittliche Größenordnung sowohl von $\omega(n)$ als auch von $\Omega(n)$ ist* $\log\log n$. *Es gibt zwei Konstanten B und B_1 mit*

$$\sum_{n\leqq x} \omega(n) = x \log\log x + Bx + o(x),$$

$$\sum_{n\leqq x} \Omega(n) = x \log\log x + B_1 x + o(x).$$

B ist die Konstante der Formel (15) *und*

$$B_1 = B + \sum_p \frac{1}{p(p-1)}.$$

Beweis.

$$\sum_{n\leqq x} \omega(n) = \sum_{n\leqq x} \sum_{p\mid n} 1 = \sum_{p\leqq x} \left[\frac{x}{p}\right] = x \sum_{p\leqq x} \frac{1}{p} + O\big(\pi(x)\big).$$

Die Formel (15) und der Primzahlsatz geben das erste Resultat.

$$\begin{aligned}\sum_{n\leqq x}\Omega(n) &= \sum_{n\leqq x}\sum_{p^\nu\mid n}1 = \sum_{p^\nu\leqq x}\left[\frac{x}{p^\nu}\right] = \sum_{n\leqq x}\omega(n) + \sum_{\substack{p^\nu\leqq x\\ \nu\geqq 2}}\left[\frac{x}{p^\nu}\right]\\ &= \sum_{n\leqq x}\omega(n) + \sum_{\substack{p^\nu\leqq x\\ \nu\geqq 2}}\frac{x}{p^\nu} + O\left(\sum_{\substack{p^\nu\leqq x\\ \nu\geqq 2}}1\right)\\ &= \sum_{n\leqq x}\omega(n) + x\left\{\sum_{\nu=2}^{\infty}\sum_{p}\frac{1}{p^\nu} + o(1)\right\} + O\left(\sqrt{x}\log x\right)\\ &= \sum_{n\leqq x}\omega(n) + x\sum_{p}\frac{1}{p(p-1)} + o(x)\\ &= x\log\log x + B_1 x + o(x).\end{aligned}$$

Wir betrachten noch einen bemerkenswerten Satz von P. Turán (1910—1976), der eine Aussage über die Abweichung von $\omega(n)$ von der durchschnittlichen Größenordnung $\log\log n$ beinhaltet. Zuvor geben wir noch die durchschnittliche Größenordnung von $\omega^2(n)$ an.

Satz 5.43. *Die durchschnittliche Größenordnung von* $\omega^2(n)$ *ist* $(\log\log n)^2$. *Es gilt*

$$\sum_{n\leqq x}\omega^2(x) = x(\log\log x)^2 + O(x\log\log x).$$

Beweis. Es bedeuten p und q jetzt stets Primzahlen. Aus

$$\omega(n)\left(\omega(n)-1\right) = \sum_{\substack{pq\mid n\\ p\neq q}}1 = \sum_{pq\mid n}1 - \sum_{p^2\mid n}1$$

ergibt sich

$$\begin{aligned}\sum_{n\leqq x}\omega^2(n) - \sum_{n\leqq x}\omega(n) &= \sum_{pqm\leqq x}1 - \sum_{p^2m\leqq x}1\\ &= \sum_{pq\leqq x}\left[\frac{x}{pq}\right] - \sum_{p^2\leqq x}\left[\frac{x}{p^2}\right]\\ &= \sum_{pq\leqq x}\frac{x}{pq} + O\Big(\sum_{pq\leqq x}1\Big) + O(x)\\ &= \sum_{pq\leqq x}\frac{x}{pq} + O\Big(\sum_{p\leqq x}\frac{x}{p}\Big) + O(x).\end{aligned}$$

Nach Satz 5.18 und Satz 5.42 folgt hieraus

$$\sum_{n\leqq x}\omega^2(n) = \sum_{pq\leqq x}\frac{x}{pq} + O(x\log\log x).$$

Zur Abschätzung der noch verbleibenden Summe beachten wir

$$\left(\sum_{p\leqq\sqrt{x}}\frac{1}{p}\right)^2=\sum_{p\leqq\sqrt{x}}\frac{1}{p}\sum_{q\leqq\sqrt{x}}\frac{1}{q}\leqq\sum_{pq\leqq x}\frac{1}{pq}\leqq\left(\sum_{p\leqq x}\frac{1}{p}\right)^2.$$

Nach Satz 5.18 ist

$$\left(\sum_{p\leqq x}\frac{1}{p}\right)^2=\big(\log\log x+O(1)\big)^2=(\log\log x)^2+O(\log\log x),$$

$$\left(\sum_{p\leqq\sqrt{x}}\frac{1}{p}\right)^2=\big(\log\log\sqrt{x}+O(1)\big)^2=(\log\log x)^2+O(\log\log x)$$

und daher

$$\sum_{n\leqq x}\omega^2(n)=x\,(\log\log x)^2+O(x\log\log x).$$

Satz 5.44 (Turán).

$$\sum_{1<n\leqq x}\big(\omega(n)-\log\log n\big)^2=O(x\log\log x).$$

Beweis. Der Teil der Summe, für den $n\leqq x^{1/6}$ ist, bringt einen Anteil von $O(x)$ und noch weniger. Für $x^{1/6}<n\leqq x$ ist

$$\log\log x-1<\log\log n\leqq\log\log x.$$

Damit ergibt sich

$$\begin{aligned}\sum_{1<n\leqq x}\big(\omega(n)-\log\log n\big)^2&=\sum_{n\leqq x}\big(\omega(n)-\log\log x\big)^2+O\Big(\sum_{n\leqq x}\omega(n)\Big)\\&\quad+O(x\log\log x)\\&=\sum_{n\leqq x}\omega^2(n)-2\log\log x\sum_{n\leqq x}\omega(n)\\&\quad+[x](\log\log x)^2+O(x\log\log x)\\&=O(x\log\log x).\end{aligned}$$

Ein interessantes Ergebnis erzielte auch R. L. Duncan, der $\Omega(n)/\omega(n)$ betrachtete.

Satz 5.45 (Duncan). *Die durchschnittliche Größenordnung von $\Omega(n)/\omega(n)$ ist* 1. *Genauer gilt*

$$\sum_{1<n\leqq x}\frac{\Omega(n)}{\omega(n)}=x+O\left(\frac{x}{\log\log x}\right).$$

Beweis. Wir führen zunächst eine Abschätzung einer Summe über $1/\omega(n)$ durch.

$$\begin{aligned}\sum_{1<n\leqq x}\frac{1}{\omega(n)} &= \sum_{\substack{1<n\leqq x\\ 2\omega(n)<\log\log x}}\frac{1}{\omega(n)} + \sum_{\substack{n\leqq x\\ 2\omega(n)\geqq\log\log x}}\frac{1}{\omega(n)}\\ &\leqq \sum_{\substack{n\leqq x\\ 2\omega(n)<\log\log x}} 1 + \frac{2x}{\log\log x}\\ &\leqq \frac{4}{(\log\log x)^2}\sum_{\substack{n\leqq x\\ 2\omega(n)<\log\log x}}\big(\omega(n)-\log\log x\big)^2 + \frac{2x}{\log\log x}\\ &\leqq \frac{4}{(\log\log x)^2}\sum_{n\leqq x}\big(\omega(n)-\log\log x\big)^2 + \frac{2x}{\log\log x}.\end{aligned}$$

Mit dem Turánschen Satz ergibt sich

$$\sum_{1<n\leqq x}\frac{1}{\omega(n)} = O\left(\frac{x}{\log\log x}\right).$$

Damit erhalten wir

$$\begin{aligned}\sum_{1<n\leqq x}\frac{\Omega(n)}{\omega(n)} &= \sum_{n\leqq x}\frac{1}{\omega(n)}\sum_{p^\nu\mid n}1 = \sum_{n\leqq x}\frac{1}{\omega(n)}\sum_{p\mid n}1 + \sum_{n\leqq x}\frac{1}{\omega(n)}\sum_{\substack{p^\nu m=n\\ \nu\geqq 2}}1\\ &= [x]-1+\sum_{\substack{p^\nu\leqq x\\ \nu\geqq 2}}\sum_{m\leqq xp^{-\nu}}\frac{1}{\omega(p^\nu m)}\\ &= x + O\left(\sum_{\substack{p^\nu\leqq x\\ \nu\geqq 2}}\sum_{m\leqq xp^{-\nu}}\frac{1}{\omega(m)}\right)\\ &= x + O\left(\sum_{m\leqq x}\frac{1}{\omega(m)}\sum_{\substack{p^\nu\leqq x/m\\ \nu\geqq 2}}1\right).\end{aligned}$$

In der zweiten Summe kann ν höchstens $O(\log x)$ Werte annehmen. Mit dem Primzahlsatz bekommen wir

$$\sum_{1<n\leqq x}\frac{\Omega(n)}{\omega(n)} = x + O\left(\sum_{m\leqq x}\frac{1}{\omega(m)}\sqrt{\frac{x}{m}}\right)$$

und mit der Abelschen Identität

$$\begin{aligned}\sum_{1<n\leqq x}\frac{\Omega(n)}{\omega(n)} &= x + O\left(\sum_{m\leqq x}\frac{1}{\omega(m)}\right) + O\left(\int_1^x t^{1/2}t^{-3/2}\sum_{m\leqq t}\frac{1}{\omega(m)}\,dt\right)\\ &= x + O\left(\frac{x}{\log\log x}\right).\end{aligned}$$

5.7.6. Die Möbiussche μ-Funktion und der Primzahlsatz

Nach Satz 5.16 und dem Primzahlsatz ist

$$\sum_{n \leqq x} \Lambda(n) = \psi(x) \sim \pi(x) \log x \sim x.$$

Demzufolge ist nachstehender Satz eine *äquivalente Formulierung des Primzahlsatzes.*

Satz 5.46. *Die durchschnittliche Größenordnung von $\Lambda(n)$ ist* 1.

Es soll eine weitere äquivalente Formulierung des Primzahlsatzes, die Aussagen über die Möbiussche μ-Funktion enthält, entwickelt werden. Dazu definieren wir:

Definition 5.18. $M(x) := \sum_{n \leqq x} \mu(n)$.

Trivial ist $M(x) = O(x)$. Die wahre Größenordnung von $M(x)$ ist nicht bekannt. Schon die Verbesserung $M(x) = o(x)$ ist ein sehr tiefliegendes Resultat, sie ist nämlich dem Primzahlsatz gleichwertig. Die beiden folgenden Sätze, die dies ausweisen werden, sollen noch durch zwei Hilfssätze vorbereitet werden.

Hilfssatz 5.6. *Für $x \geqq 1$ gilt*

$$\left| \sum_{n \leqq x} \frac{\mu(n)}{n} \right| \leqq 1.$$

Beweis. Aus $1 * \mu(n) = \varepsilon(n)$ folgt für $x \geqq 1$

$$\sum_{n \leqq x} \mu(n) \left[\frac{x}{n} \right] = 1.$$

Daher ist

$$\begin{aligned} x \sum_{n \leqq x} \frac{\mu(n)}{n} &= \sum_{n \leqq x} \mu(n) \left\{ \frac{x}{n} - \left[\frac{x}{n} \right] \right\} + \sum_{n \leqq x} \mu(n) \left[\frac{x}{n} \right] \\ &= x - [x] + 1 + \sum_{2 \leqq n \leqq x} \mu(n) \left\{ \frac{x}{n} - \left[\frac{x}{n} \right] \right\} \end{aligned}$$

und

$$\left| x \sum_{n \leqq x} \frac{\mu(n)}{n} \right| \leqq x - [x] + 1 + \sum_{2 \leqq n \leqq x} \left\{ \frac{x}{n} - \left[\frac{x}{n} \right] \right\} < x.$$

Hilfssatz 5.7. $M(x) \log x = -\sum_{n \leqq x} \mu(n)\, \psi\left(\frac{x}{n}\right) + O(x)$.

Beweis. Nach Hilfssatz 5.1 und Definition 5.6 ist

$$\begin{aligned} M(x) \log x &= \sum_{n \leqq x} \mu(n) \log n + \sum_{n \leqq x} \mu(n) \log \frac{x}{n} \\ &= \sum_{n \leqq x} \mu(n) \sum_{t \mid n} \Lambda(t) + O(x) \\ &= \sum_{t \leqq x} \Lambda(t) \sum_{d \leqq x/t} \mu(t \cdot d) + O(x). \end{aligned}$$

Nun ist $\Lambda(t) = \log p$ für $t = p^\nu$ und sonst 0. Und $\mu(t \cdot d)$ ist höchstens dann von 0 verschieden, wenn $\nu = 1$ ist. Daher ist

$$\begin{aligned} M(x) \log x &= \sum_{p \leqq x} \log p \sum_{d \leqq x/p} \mu(pd) + O(x) \\ &= -\sum_{p \leqq x} \log p \; M\left(\frac{x}{p}\right) + \sum_{p \leqq x} \log p \sum_{d \leqq x/p^2} \mu(d) + O(x) \\ &= -\sum_{n \leqq x} \Lambda(n) \; M\left(\frac{x}{n}\right) + O(x) \\ &= -\sum_{n \leqq x} \mu(n) \, \psi\left(\frac{x}{n}\right) + O(x). \end{aligned}$$

Satz 5.47. *Aus dem Primzahlsatz folgt* $M(x) = o(x)$.

Beweis. Nach Hilfssatz 5.7 ist

$$\sum_{n \leqq x} \mu(n) \, \psi\left(\frac{x}{n}\right) = o(x \log x)$$

zu zeigen. In Anwendung des Primzahlsatzes $\psi(x) \sim x$ können wir zu jedem $\varepsilon > 0$ ein $x_0 > 0$ bestimmen mit $|\psi(x) - x| < \varepsilon x$ für $x \geqq x_0$. Mit diesem x_0 zerlegen wir für $x > x_0$ die Summe in

$$\sum_{n \leqq x} \mu(n) \, \psi\left(\frac{x}{n}\right) = \sum_{n \leqq x/x_0} \mu(n) \, \psi\left(\frac{x}{n}\right) + \sum_{x/x_0 < n \leqq x} \mu(n) \, \psi\left(\frac{x}{n}\right).$$

Für die erste Teilsumme ist dann unter Ausnutzung von Hilfssatz 5.6

$$\begin{aligned} \left| \sum_{n \leqq x/x_0} \mu(n) \, \psi\left(\frac{x}{n}\right) \right| &\leqq x \left| \sum_{n \leqq x/x_0} \frac{\mu(n)}{n} \right| + \sum_{n \leqq x/x_0} \left| \psi\left(\frac{x}{n}\right) - \frac{x}{n} \right| \\ &< x + \varepsilon \sum_{n \leqq x/x_0} \frac{x}{n} < x + \varepsilon x (1 + \log x) \\ &< 2x + \varepsilon x \log x, \end{aligned}$$

sofern man $\varepsilon < 1$ annimmt. Die Abschätzung der zweiten Teilsumme ergibt

$$\left| \sum_{x/x_0 < n \leqq x} \mu(n) \, \psi\left(\frac{x}{n}\right) \right| \leqq \sum_{x/x_0 < n \leqq x} \psi\left(\frac{x}{n}\right) \leqq \psi(x_0) \, x.$$

Insgesamt ergibt sich

$$\left| \sum_{n \leqq x} \mu(n) \, \psi\left(\frac{x}{n}\right) \right| < \big(2 + \psi(x_0)\big) \, x + \varepsilon x \log x.$$

Weiter gibt es ein $x_1 \geqq x_0$ mit $2 + \psi(x_0) < \varepsilon \log x$ für $x > x_1$, so daß

$$\left| \sum_{n \leqq x} \mu(n) \, \psi\left(\frac{x}{n}\right) \right| < 2\varepsilon x \log x$$

ist. Das war zu zeigen.

Satz 5.48. *Aus $M(x) = o(x)$ folgt der Primzahlsatz.*

Beweis. Wir bilden mit der Teilerfunktion $d(n)$ und der Eulerschen Konstanten C die Funktion

$$f(n) := \log n - d(n) + 2C.$$

Auf Grund der Beziehungen $\Lambda(n) = \mu(n) * \log n$, $\mu(n) * d(n) = 1$, $\mu(n) * 1 = \varepsilon(n)$ ist

$$\begin{aligned}\psi(x) - [x] + 2C &= \sum_{n \leqq x} \{\Lambda(n) - 1 + 2C\varepsilon(n)\} \\ &= \sum_{n \leqq x} \sum_{t \mid n} \mu(t) f\left(\frac{n}{t}\right) \\ &= \sum_{mn \leqq x} \mu(m) f(n).\end{aligned}$$

Zum Nachweis des Primzahlsatzes in der Form $\psi(x) \sim x$ ist zu zeigen, daß die Summe $o(x)$ für $x \to \infty$ ist. Mit

$$F(x) := \sum_{n \leqq x} f(n)$$

und $y < \sqrt{x}$ zerlegen wir die Summe in

$$\begin{aligned}\sum_{mn \leqq x} \mu(m) f(n) &= \sum_{m \leqq x/y} \mu(m) \sum_{n \leqq x/m} f(n) + \sum_{\substack{mn \leqq x \\ x/y < m \leqq x}} \mu(m) f(n) \\ &= \sum_{m \leqq x/y} \mu(m) F\left(\frac{x}{m}\right) + \sum_{n \leqq y} f(n) M\left(\frac{x}{n}\right) - F(y) M\left(\frac{x}{y}\right). \qquad (27)\end{aligned}$$

Auf Grund der Stirlingschen Formel und des Satzes 5.39 ist

$$F(x) = (x \log x - x) - \left(x \log x + (2C - 1)x\right) + 2Cx + O\left(\sqrt{x}\right) = O\left(\sqrt{x}\right),$$

so daß es eine Konstante $A_1 > 0$ mit $|F(x)| \leqq A_1 \sqrt{x}$ für $x \geqq 1$ gibt. Dann gibt es auch eine Konstante A_2 mit

$$\left| \sum_{m \leqq x/y} \mu(m) F\left(\frac{x}{m}\right) \right| \leqq A_1 \sum_{m \leqq x/y} \sqrt{\frac{x}{m}} \leqq A_2 \frac{x}{\sqrt{y}}. \qquad (28)$$

Aus der trivialen Abschätzung $M(x) = O(x)$ folgt die Existenz einer Konstanten $A_3 > 0$ mit

$$\left| F(y) M\left(\frac{x}{y}\right) \right| \leqq A_3 \frac{x}{\sqrt{y}}. \qquad (29)$$

Zur Abschätzung der zweiten Summe in (27) bemerken wir, daß wir infolge der Bedingung $M(x) = o(x)$ zu gegebenem, beliebig großem y das x so groß wählen können, daß

$$\max_{n \leqq y} \left| M\left(\frac{x}{n}\right) \right| < \frac{x}{y^2}$$

ausfällt. Somit gibt es eine Konstante $A_4 > 0$ mit

$$\left| \sum_{n \leqq y} f(n)\, M\left(\frac{x}{n}\right) \right| < \frac{x}{y^2} \sum_{n \leqq y} |f(n)| \leqq \frac{x}{y^2} \sum_{n \leqq y} \left(\log n + d(n) + 2C\right)$$

$$\leqq A_4 \frac{x}{y} \log y. \tag{30}$$

Verwendet man (28), (29) und (30) in (27), so erhält man

$$\left| \sum_{mn \leqq x} \mu(m)\, f(n) \right| \leqq \left(\frac{A_2 + A_3}{\sqrt{y}} + A_4 \frac{\log y}{y} \right) x < \varepsilon x$$

für hinreichend großes y.

5.8. Die normale Größenordnung zahlentheoretischer Funktionen

Definition 5.19. Es sei E eine Eigenschaft natürlicher Zahlen. Die zahlentheoretische Funktion $a_E(n)$ sei erklärt durch:
$a_E(n) = 1$, falls n die Eigenschaft E hat; $a_E(n) = 0$, falls n die Eigenschaft E nicht hat. Ist

$$A_E(x) := \sum_{n \leqq x} a_E(n) \sim x \qquad (x \to \infty),$$

so sagen wir: *Fast alle natürlichen Zahlen haben die Eigenschaft E.*

Satz 5.49. *Fast alle natürlichen Zahlen sind zusammengesetzt.*

Beweis. E bedeutet hier, n ist zusammengesetzt. Dann ist

$$[x] = 1 + A_E(x) + \pi(x).$$

Nach dem Primzahlsatz ist $\pi(x) = o(x)$ und daher $A_E(x) \sim x$.

Dieser Satz beinhaltet also nur eine andere Formulierung eines uns bekannten Sachverhaltes. Jetzt beschäftigen wir uns mit Aussagen über die Funktionen $\omega(n)$, $\Omega(n)$, $d(n)$.

Satz 5.50 *Für beliebiges $\delta > 0$ besteht die Ungleichung*

$$|\omega(n) - \log\log n| < (\log\log n)^{1/2+\delta} \tag{31}$$

für fast alle natürlichen Zahlen n.

Beweis. E bezeichne die Eigenschaft von n, die Ungleichung (31) zu erfüllen. Es ist

$$[x] - A_E(x) = \sum_{n \leqq x} \left(1 - a_E(n)\right).$$

Da für $e^e \leqq x^{1/e} < n$ die Ungleichung

$$\log\log x < \log\log n + 1 \leqq 2 \log\log n$$

besteht, erhalten wir

$$(\log\log x)^{1+2\delta}\big([x]-A_E(x)\big)$$
$$<\sum_{2<n\leqq x}\big(1-a_E(n)\big)\,(2\log\log n)^{1+2\delta}+O\big(x^{1/e}\,(\log\log x)^{1+2\delta}\big).$$

Das Restglied können wir durch $O(x)$ abschätzen. Für $a_E(n)=1$ sind die entsprechenden Summanden 0, für $a_E(n)=0$ gilt die Ungleichung (31) nicht. Daher ist bei Berücksichtigung des Satzes von TURÁN

$$(\log\log x)^{1+2\delta}\big([x]-A_E(x)\big)$$
$$<2^{1+2\delta}\sum_{2<n\leqq x}\big(1-a_E(n)\big)\,\big(\omega(n)-\log\log n\big)^2+O(x)$$
$$\leqq 2^{1+2\delta}\sum_{2<n\leqq x}\big(\omega(n)-\log\log n\big)^2+O(x)=O(x\log\log x).$$

Daraus ergibt sich

$$x-A_E(x)=O\big(x(\log\log x)^{-2\delta}\big)$$

und $A_E(x)\sim x$.

Satz 5.51. *Für beliebige $\delta>0$ besteht die Ungleichung*

$$|\Omega(n)-\log\log n|<(\log\log n)^{1/2+\delta}$$

für fast alle natürlichen Zahlen n.

Beweis. Nach Satz 5.42 ist

$$\sum_{n\leqq x}\big(\Omega(n)-\omega(n)\big)=O(x).$$

Bezeichnet E die Eigenschaft

$$\Omega(n)-\omega(n)<(2\log\log n)^{1/2}, \tag{32}$$

so können wir die Summe wegen $\Omega(n)-\omega(n)\geqq 0$ durch

$$\sum_{n\leqq x}\big(1-a_E(n)\big)\,\big(\Omega(n)-\omega(n)\big)\leqq\sum_{n\leqq x}\big(\Omega(n)-\omega(n)\big)=O(x)$$

abschätzen. Für $n>x^{1/e}\geqq e^e$ ist $2\log\log n\geqq\log\log x$, und daher ist

$$\big([x]-A_E(x)\big)\,(\log\log x)^{1/2}\leqq\sum_{1<n\leqq x}\big(1-a_E(n)\big)\,(2\log\log n)^{1/2}+O(x)$$
$$\leqq\sum_{n\leqq x}\big(1-a_E(n)\big)\,\big(\Omega(n)-\omega(n)\big)+O(x)=O(x).$$

Folglich ist

$$A_E(x)=x+O\big(x(\log\log x)^{-1/2}\big),$$

und die Ungleichung (32) gilt für fast alle n. Somit gilt auch für fast alle n und mit $\delta > \delta_0 > 0$ bei Verwendung von Satz 5.50

$$\begin{aligned}|\Omega(n) - \log\log n| &\leqq |\omega(n) - \log\log n| + \Omega(n) - \omega(n)\\ &< (\log\log n)^{1/2+\delta_0} + (2\log\log n)^{1/2}\\ &< (\log\log n)^{1/2+\delta}.\end{aligned}$$

Diese beiden Sätze nehmen wir zum Anlaß, den Begriff der normalen Größenordnung einzuführen.

Definition 5.20. Die zahlentheoretische Funktion $f(n)$ hat die *normale Größenordnung* $g(n)$, wenn für jedes positive ε die Ungleichung

$$|f(n) - g(n)| < \varepsilon g(n)$$

für fast alle n gilt.

Damit ergibt sich aus den vorangegangenen Sätzen sofort der folgende Satz.

Satz 5.52 (Hardy/Ramanujan). *Beide Funktionen $\omega(n)$ und $\Omega(n)$ besitzen die normale Größenordnung* $\log\log n$.

Satz 5.53. *Die normale Größenordnung von $\Omega(n)/\omega(n)$ ist* 1.

Beweis. Da die Ungleichung (32) für fast alle n gilt, erhalten wir mit Satz 5.52, $0 < \varepsilon' < 1$, $\varepsilon > 0$ für fast alle n

$$0 \leqq \frac{\Omega(n)}{\omega(n)} - 1 \leqq \frac{1}{1-\varepsilon'}\left(\frac{2}{\log\log n}\right)^{1/2} < \varepsilon.$$

Satz 5.54 (Hardy/Ramanujan). *Die normale Größenordnung von* $\log d(n)$ *ist* $\log 2 \cdot \log\log n$. *Das heißt, für beliebiges $\varepsilon > 0$ besteht die Ungleichung*

$$2^{(1-\varepsilon)\log\log n} < d(n) < 2^{(1+\varepsilon)\log\log n}$$

für fast alle n.

Beweis. Für

$$n = \prod_{i=1}^{r} p_i^{\nu_i}$$

ist $\omega(n) = r$, $\Omega(n) = \nu_1 + \nu_2 + \cdots + \nu_r$, $d(n) = (1+\nu_1)(1+\nu_2)\cdot\cdots\cdot(1+\nu_r)$. Wegen $2 \leqq 1 + \nu \leqq 2^\nu$ für $\nu \geqq 1$ ist

$$2^{\omega(n)} \leqq d(n) \leqq 2^{\Omega(n)}.$$

Nach Satz 5.52 ist

$$(1-\varepsilon)\log\log n < \omega(n) \leqq \frac{\log d(n)}{\log 2} \leqq \Omega(n) < (1+\varepsilon)\log\log n$$

für fast alle n. Daraus folgt der Satz.

Zusammenfassend können wir feststellen, daß die normale Größenordnung $\log\log n$ von $\omega(n)$ und $\Omega(n)$ mit der durchschnittlichen Größenordnung übereinstimmt. Selbst für den Quotienten $\Omega(n)/\omega(n)$ sind durchschnittliche und normale Größenordnung gleich 1. Das zeigt einerseits, daß $\omega(n)$ und $\Omega(n)$ ein „regelmäßigeres" Verhalten zeigen, als zunächst angenommen werden konnte und andererseits, daß sich beide Funktionen gar nicht so erheblich unterscheiden.

Anders sieht es dagegen mit der Teilerfunktion aus. Man kann zwar im Sinne der Definition nicht sagen, daß die normale Größenordnung von $d(n)$

$$2^{\log\log n} = (\log n)^{\log 2}$$

wäre. Dennoch zeigt der Satz, daß sich $d(n)$ im wesentlichen in der Nähe dieses Wertes bewegt. Da $\log 2 = 0{,}69\ldots$ ist, unterscheidet sich dieser Wert von der durchschnittlichen Größenordnung $\log n$. Wenige Werte von n, für die $d(n)$ abnorm groß wird, bewirken diese Abweichung der durchschnittlichen Größenordnung von $(\log n)^{\log 2}$.

5.9. Aufgaben

1. Man beweise $1 * d^3(n) = (1 * d(n))^2$.
2. Man beweise $\sigma_1(n) = \varphi(n) * \sigma_0(n)$.
3. Man beweise $\sigma_k{}^2(n) = n^k * \sigma_k(n^2)$.
4. Die Liouvillesche Funktion $\lambda(n)$ ist durch $\lambda(1) = 1$ und
   $\lambda(n) = (-1)^{\Omega(n)}$ $(n > 1)$ erklärt. Man zeige
   a) $1 * \lambda(n) = \begin{cases} 1 & \text{für } n = a^2, \\ 0 & \text{sonst,} \end{cases}$
   b) $\lambda^{-1}(n) = |\mu(n)|$,
   c) $\lambda(n) = \sum_{t^2 \mid n} \mu\left(\frac{n}{t^2}\right)$,
   d) $\sum_{n \leqq x} \lambda(n)\left[\frac{x}{n}\right] = \left[\sqrt{x}\right]$.
5. Es sei $h(x)$ eine beliebige, für alle rationalen x in $0 \leqq x \leqq 1$ erklärte Funktion. Für die Funktionen
   $$g(n) = \sum_{r=1}^{n} h\left(\frac{r}{n}\right), \qquad f(n) = \sum_{\substack{r \leqq n \\ (r,n)=1}} h\left(\frac{r}{n}\right)$$
   besteht dann der Zusammenhang $f(n) = \mu(n) * g(n)$.
6. Mit Hilfe des Ergebnisses von Aufgabe 5 leite man
   $$\mu(n) = \sum_{\substack{r \leqq n \\ (r,n)=1}} e^{2\pi i \frac{r}{n}}$$
   her.
7. $f(n)$ und $g(n)$ seien zwei beliebige zahlentheoretische Funktionen. Die zahlentheoretische Funktion $\lambda_k(n)$ werde für $k = 2, 3, \ldots$ erklärt durch
   (1) $\lambda_k(n)$ ist multiplikativ,
   (2) für Primzahlen p und ganze Zahlen a, b mit $a \geqq 0$, $0 \leqq b < k$ ist
   $$\lambda_k(p^{ak+b}) = \begin{cases} +1 & \text{für } b = 0, \\ -1 & \text{für } b = 1, \\ 0 & \text{für } 2 \leqq b < k. \end{cases}$$

Weiterhin sei $q_k(n)$ gleich 0, falls n durch die k-te Potenz ($k \geqq 2$) einer Primzahl teilbar ist, andernfalls gleich 1. Man zeige: Es ist $g(n) = \lambda_k(n) * f(n)$ genau dann, wenn $f(n) = q_k(n) * g(n)$. — E. Krätzel.

8. Unter Verwendung der Polynome a) $x^2 + 1$, b) $4x - 1$, c) $x^2 + 3$, d) $6x - 1$ zeige man: Es gibt unendlich viele Primzahlen der Gestalt a) $p \equiv 1 \pmod 4$, b) $p \equiv 3 \pmod 4$, c) $p \equiv 1 \pmod 6$, d) $p \equiv 5 \pmod 6$.
9. Man beweise $d(n) \leqq 2\sqrt{n}$. — W. Sierpiński.
10. Für zusammengesetztes n weise man $\sigma(n) > n + \sqrt{n}$ nach. — W. Sierpiński.
11. Für $n > 2$ ist $\sigma(n) < n\sqrt{n}$ zu zeigen. — C. C. Lindner.
12. Man zeige: Es ist $\varphi(n)\, d(n) \geqq n$, wobei das Gleichheitszeichen genau für $n = 1, 2$ steht. — R. Sivaramakrishnan.
13. Man zeige: Für $n \neq 4$ ist $\varphi(n)\, d^2(n) \leqq n^2$, wobei das Gleichheitszeichen genau für $n = 1, 2, 8, 12$ steht. — S. Porubski.
14. Man zeige: Er ist $\sigma(n) \leqq \dfrac{n+1}{2}\, d(n)$, wobei das Gleichheitszeichen genau im Falle einer Primzahl $n = p$ steht. — E. S. Langford.
15. Für $n > 1$ ist

$$\frac{\sigma(n)}{n} < \begin{cases} \left(\dfrac{3}{2}\right)^{\omega(n)} & \text{für} \quad n \equiv 1 \pmod 2, \\ 2\left(\dfrac{3}{2}\right)^{\omega(n)} & \text{für} \quad n \equiv 0 \pmod 2 \end{cases}$$

nachzuweisen. — M. Satyanarayana.

16. Man beweise $d^2(n)\, \varphi(n) > \sigma(n)$ für $n > 1$. — A. Makowski.
17. Für beliebige natürliche Zahlen k, n weise man $\sigma_k(n) \geqq n^{k/2}\, d(n)$ nach. — S. Sivaramakrishnan, C. S. Venkataraman.
18. Für $r = 1, 2, \ldots$ bezeichne $(n, m)_r$ den größten gemeinsamen Teiler von n und m der Potenz r und $c_m^{(r)}(a)$ die verallgemeinerte Ramanujansche Summe

$$c_m^{(r)}(a) = \sum_{\substack{n=1 \\ (n, m^r)_r = 1}}^{m^r} e^{2\pi i a n m^{-r}}.$$

Man zeige

$$c_m^{(r)}(a) = \sum_{t \mid m, t^r \mid a} t^r \mu\left(\frac{m}{t}\right).$$

19. Für $r = 1, 2, \ldots$ und beliebige reelle k bezeichne $\sigma_k(r, m)$ die Teilerfunktion

$$\sigma_k(r, n) = \sum_{t d^r = n} t^k.$$

Mit Hilfe des Ergebnisses von Aufgabe 18 beweise man für $k > \dfrac{1}{r} - 1$

$$\sigma_k(r, n) = \zeta(kr + r)\, n^k \sum_{m=1}^{\infty} \frac{c_m^{(r)}(n)}{m^{kr+r}}.$$

— E. Krätzel.

20. Für natürliche Zahlen n, m sei

$$\gamma(n, m) = \begin{cases} 1 & \text{für} \quad (n, m) = 1, \\ \prod\limits_{\substack{p \mid n \\ p \mid m}} (1 - p) & \text{für} \quad (n, m) > 1. \end{cases}$$

Man zeige

$$\gamma(n, m) = \sum_{t \mid n, t \mid m} t \mu(t).$$

— E. Krätzel.

21. Mit Hilfe des Ergebnisses von Aufgabe 20 beweise man

$$J_k(n) = \frac{n^k}{\zeta(k+1)} \sum_{m=1}^{\infty} \frac{\gamma(m, n)}{m^{k+1}}$$

für $k = 1, 2, \ldots$ — E. Krätzel.

22. Es sei für $k = 1, 2, \ldots$

$$F_k(x) = \sum_{1 \leqq m \leqq n \leqq x} (m, n)^k.$$

Man beweise

a) $F_1(x) = \frac{x^2 \log x}{2\zeta(2)} + O(x^2)$,

b) $F_2(x) = \frac{\zeta(2)\, x^3}{3\zeta(3)} + O(x^2 \log x)$,

c) $F_k(x) = \frac{\zeta(k)\, x^{k+1}}{(k+1)\,\zeta(k+1)} + O(x^k)$ für $k > 2$.

— E. Teuffel.

23. Man beweise die Verschärfung von Aufgabe 22a)

$$F_1(x) = \frac{x^2}{2\zeta(2)} (\log x + A) + O(x^{3/2} \log x),$$

wobei A eine geeignete Konstante bedeutet. — E. Krätzel.

6. Gitterpunkte

Diejenigen Punkte eines n-dimensionalen euklidischen Raumes, die bezüglich eines kartesischen Koordinatensystems ganzzahlige Koordinaten besitzen, heißen Gitterpunkte. Wir beschäftigen uns mit der Abzählung solcher Gitterpunkte auf Kurven und Flächen in abgeschlossenen Bereichen. Diese an sich geometrische Fragestellung ist tatsächlich ein zahlentheoretisches Problem. Rein äußerlich erkennt man dies schon daran, daß es sich um die Beschäftigung mit ganzen Zahlen handelt. Oftmals hängt es nur vom Standpunkt der Betrachtungsweise ab, ob man ein Problem als geometrisches oder zahlentheoretisches ansieht. So ist beispielsweise die Frage nach der Anzahl der Gitterpunkte auf dem Kreis $x^2 + y^2 = n$ äquivalent zur Frage nach der Anzahl der Darstellungen der natürlichen Zahl n als Summe von zwei Quadraten.

Wir werden bis auf wenige Ausnahmen hauptsächlich zweidimensionale Probleme betrachten. Wir beginnen mit den Gitterpunkten auf Kurven zweiter Ordnung. Die Problematik wird für Parabeln ganz einfach, für Hyperbeln lösbar, für Ellipsen dagegen schwierig sein, so daß der Fall der Ellipsen nur beispielhaft abgehandelt werden kann. In den Abschnitten 6.3 und 6.4 betrachten wir allgemeiner statt Gitterpunkte rationale Punkte, also solche mit rationalen Koordinaten. Für Kurven zweiter Ordnung erhalten wir ein vollständig befriedigendes Ergebnis, für höhere Kurven werden nur ein paar Spezialfälle betrachtet.

In Abschnitt 6.5 behandeln wir das allgemeine Problem der Abschätzung der Anzahl der Gitterpunkte in ebenen Bereichen. Einige Spezialfälle haben wir bei der Untersuchung der durchschnittlichen Größenordnung der Funktionen $r(n)$ und $d(n)$ bereits kennengelernt. Die dort erzielten Abschätzungen werden vermöge einer von I. M. Vinogradov entwickelten Methode verbessert.

6.1. Gitterpunkte auf Kurven zweiter Ordnung

Gegeben sei eine nicht zerfallende, reelle Kurve zweiter Ordnung

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \tag{1}$$

mit ganzzahligen Koeffizienten $a, \ldots, f$. Wir fragen, ob eine solche Kurve Gitterpunkte enthält oder nicht. Es ist zweckmäßig, die Fälle der Parabel, Ellipse, Hyperbel getrennt zu behandeln.

6.1.1. Gitterpunkte auf Parabeln

Die Kurve (1) stelle eine Parabel dar, so daß $b^2 - 4ac = 0$ ist. Mindestens einer der Koeffizienten a, c muß verschieden von 0 sein. Wir nehmen $a \neq 0$ an. Durch Multiplikation von (1) mit $4a$ und Einsetzen von $4ac = b^2$ erhalten wir aus (1)

$$(2ax + by)^2 + 4adx + 4aey + 4af = 0.$$

Die Transformation

$$x' = 2ax + by, \qquad y' = y \tag{2}$$

führt die Parabel (1) in die Parabel

$$x'^2 + 2dx' + 2(2ae - bd)\, y' + 4af = 0$$

über, wobei natürlich $2ae - bd \neq 0$ sein muß. Auf der neuen Parabel liegen genau dann, und zwar unendlich viele Gitterpunkte, wenn die quadratische Kongruenz

$$x'^2 + 2dx' + 4af \equiv 0 \quad (|4ae - 2bd|)$$

lösbar ist. Die Transformation (2) ist so beschaffen, daß jeder Gitterpunkt von (1) wieder in einen Gitterpunkt übergeht. Die Umkehrung gilt aber nicht. Hat jedoch das System (2) wenigstens eine Lösung in ganzen Zahlen x, y, so gleich unendlich viele. Damit haben wir:

Satz 6.1. *Auf einer Parabel mit ganzzahligen Koeffizienten liegen entweder keine oder unendlich viele Gitterpunkte.*

Beispiele:

1. $4x^2 + 12xy + 9y^2 - 3y - 1 = 0.$

Die Transformation

$$x' = 2x + 3y, \qquad y' = y \tag{3}$$

führt die Parabel über in

$$x'^2 - 3y' - 1 = 0.$$

Auf dieser Parabel liegen die beiden Gitterpunktscharen

$$x_1' = 1 + 3k_1, \qquad y_1' = 3k_1^2 + 2k_1,$$
$$x_2' = -1 + 3k_2, \qquad y_2' = 3k_2^2 - 2k_2$$

mit $k_1, k_2 \in \mathbf{Z}$. Die Ausgangsparabel enthält dagegen keinen einzigen Gitterpunkt, da das System (3) in ganzen Zahlen nicht lösbar ist.

2. $4x^2 + 12xy + 9y^2 - 3y - 4 = 0.$

Die Transformation (3) gibt

$$x'^2 - 3y' - 4 = 0$$

mit den beiden Gitterpunktscharen

$$x_1' = 1 + 3k_1, \qquad y_1' = 3k_1^2 + 2k_1 - 1,$$
$$x_2' = -1 + 3k_2, \qquad y_2' = 3k_2^2 - 2k_2 - 1.$$

Die Rücktransformation liefert über (3) für die vorgegebene Parabel die beiden Gitterpunktscharen

$$x_1 = 2 - \frac{3k_1 + 9k_1^2}{2}, \qquad y_1 = -1 + 2k_1 + 3k_1^2,$$

$$x_2 = 1 + \frac{9k_2 - 9k_2^2}{2}, \qquad y_2 = -1 - 2k_2 + 3k_2^2.$$

6.1.2. Gitterpunkte auf Ellipsen

Zu Beginn betrachten wir noch Ellipsen und Hyperbeln gemeinsam. In der Darstellung (1) ist dann $4ac - b^2 \neq 0$. Ist $a = c = 0$, so muß $b \neq 0$ sein. Die Transformation

$$x' = b(x + y) + d + e, \qquad y' = b(x - y) - d + e \tag{4}$$

bringt für diesen Fall die Hyperbel (1) in die Gestalt

$$x'^2 - y'^2 = N$$

mit $N = 4de - 4bf \neq 0$. Ist etwa $c \neq 0$, so multiplizieren wir (1) mit $4c(4ac - b^2)$ und führen die Transformation

$$x' = (4ac - b^2)\,x + 2dc - be, \qquad y' = bx + 2cy + e \tag{5}$$

aus. Wir erhalten eine Gleichung der Gestalt

$$x'^2 + (4ac - b^2)\,y'^2 = M, \qquad M \neq 0.$$

Mit den Abkürzungen $D := |4ac - b^2|$, $N := |M|$ bekommen wir für $4ac - b^2 > 0$ und $M > 0$ die reelle Ellipse

$$x'^2 + Dy'^2 = N$$

und für $4ac - b^2 < 0$ die Hyperbeln

$$x'^2 - Dy'^2 = \pm N.$$

Die Transformationen (4) und (5) führen wieder Gitterpunkte in Gitterpunkte über, so daß wir uns auf die Behandlung von Ellipsen und Hyperbeln des transformierten Typs beschränken können.

Hinsichtlich der Ellipsen betrachten wir jetzt einige Spezialfälle.

Satz 6.2. *Es sei p eine Primzahl. Auf der Ellipse $x^2 + Dy^2 = p$, $D \neq p$, liegen entweder keine oder für $D > 1$ genau vier und für $D = 1$ genau acht Gitterpunkte.*

Äquivalente Formulierung: *Die Darstellung einer Primzahl p in der Form $p = x^2 + Dy^2$ mit natürlichen Zahlen x, y ist, wenn überhaupt möglich, für $D > 1$ eindeutig und für $D = 1$ auch, sofern man von der Reihenfolge der Summanden absieht.*

Beweis. Wir nehmen an, p besitzt die beiden Darstellungen

$$p = x^2 + Dy^2 = x_1^2 + Dy_1^2$$

mit $x, y, x_1, y_1 \in \mathbf{N}$ und $(x, y) = (x_1, y_1) = 1$. Für p^2 haben wir dann

$$\begin{aligned} p^2 &= (x^2 + Dy^2)(x_1^2 + Dy_1^2) = (xx_1 + Dyy_1)^2 + D(xy_1 - x_1y)^2 \\ &= (xx_1 - Dyy_1)^2 + D(xy_1 + x_1y)^2. \end{aligned}$$

Aus

$$\begin{aligned} (xx_1 + Dyy_1)(xy_1 + x_1y) &= (x^2 + Dy^2)x_1y_1 + (x_1^2 + Dy_1^2)xy \\ &= p(x_1y_1 + xy) \end{aligned}$$

folgt, daß p wenigstens einen der beiden Faktoren der linken Seite teilt: Ist $p \mid (xx_1 + Dyy_1)$, so ist $xy_1 - x_1y = 0$ und $x = x_1$, $y = y_1$, und beide Lösungen sind identisch. Ist aber $p \mid (xy_1 + x_1y)$, so ist $p^2 \geqq Dp^2$, was für $D > 1$ unmöglich ist. Für $D = 1$ ist dann $xx_1 - yy_1 = 0$ und $x = y_1$, $y = x_1$. Das beweist den Satz.

Satz 6.3. *Jede Primzahl $p \equiv 1$ (4) kann in der Form $p = x^2 + y^2$ mit natürlichen Zahlen x, y dargestellt werden. Für Primzahlen $p \equiv 3$ (4) besteht eine solche Darstellung nicht.*

Beweis. Besteht eine Darstellung $p = x^2 + y^2$, so ist $(x, y) = 1$. Da auch $(y, p) = 1$ ist, gibt es ein z mit $yz \equiv x$ (p). Daher ist

$$x^2 + y^2 \equiv y^2(z^2 + 1) \equiv 0 \quad (p),$$

und $z^2 \equiv -1$ (p) ist eine notwendige Bedingung für die Darstellbarkeit von p. Diese Kongruenz ist wegen $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ für $p \equiv 1$ (4) lösbar und für $p \equiv 3$ (4) unlösbar.

Es sei jetzt $p \equiv 1$ (4) und z eine Lösung von $z^2 \equiv -1$ (p). Nach Satz 4.7 gibt es zu $\frac{z}{p}$ und $\sqrt{p}$ eine Zahl $\frac{a}{y}$, $(a, y) = 1$, mit $1 \leqq y \leqq \sqrt{p}$ und

$$\left| \frac{z}{p} + \frac{a}{y} \right| < \frac{1}{y\sqrt{p}}.$$

Setzt man $yz + ap = x$, so ist $yz \equiv x(p)$ und $|x| < \sqrt{p}$. Für diese Zahlen x, y gilt

$$x^2 + y^2 \equiv y^2(z^2 + 1) \equiv 0 \quad (p).$$

Wegen $0 < x^2 + y^2 < 2p$ ist $x^2 + y^2 = p$ die gewünschte Darstellung von p.

Satz 6.4. *Jede Primzahl $p \equiv 1$ (6) kann in der Form $p = x^2 + 3y^2$ mit natürlichen Zahlen x, y dargestellt werden. Für Primzahlen $p \equiv -1$ (6) besteht eine solche Darstellung nicht.*

Beweis. Analog zum Beweis des Satzes 6.3 findet man als notwendige Bedingung $z^2 \equiv -3 \pmod{p}$. Aus

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = \begin{cases} 1 & \text{für } p \equiv 1 \pmod{6}, \\ -1 & \text{für } p \equiv -1 \pmod{6} \end{cases}$$

ergibt sich die Möglichkeit einer Darstellung für p nur für $p \equiv 1 \pmod{6}$. Für $p \equiv 1 \pmod{6}$ sei z eine Lösung von $z^2 \equiv -3 \pmod{p}$. Wir bestimmen über Satz 4.7 zu $\frac{z}{p}$ und $\sqrt{p}$ eine Zahl $\frac{a}{y}$, $(a, y) = 1$, mit $1 \leqq y \leqq \sqrt{p}$ und

$$\left| \frac{z}{p} + \frac{a}{y} \right| < \frac{1}{y\sqrt{p}}.$$

Für die Zahl $x = yz + ap$ gilt $x \equiv yz \pmod{p}$ und $|x| < \sqrt{p}$. Folglich ist

$$x^2 + 3y^2 \equiv y^2(z^2 + 3) \equiv 0 \pmod{p},$$

und wegen $0 < x^2 + 3y^2 < 4p$ ist $x^2 + 3y^2 = mp$ mit den möglichen Werten $m = 1, 2, 3$. Da stets $x^2 + 3y^2 \not\equiv 2 \pmod{4}$ ist, scheidet die Möglichkeit $m = 2$ aus. Für $m = 3$ muß x durch 3 teilbar sein, und mit $x = 3x_1$ erhält man wie im Fall $m = 1$ eine gewünschte Gleichung $3x_1^2 + y^2 = p$.

Satz 6.5. *Auf dem Kreis $x^2 + y^2 = n$, $n > 1$, liegen genau dann Gitterpunkte, wenn jeder Primfaktor von n der Gestalt $4m + 3$ in der kanonischen Zerlegung von n einen geraden Exponenten besitzt.*

Beweis. Die Bedingung ist notwendig: Es sei n darstellbar, $n = x^2 + y^2$, mit $(x, y) = d$. Wir setzen $x = dx_1$, $y = dy_1$. Dann ist $(x_1, y_1) = 1$ und $d^2 \mid n$, und es ergibt sich mit $n = d^2 n_1$ die Darstellung $n_1 = x_1^2 + y_1^2$. Nun sei p ein Primteiler von n mit $p^{2k-1} \mid n$ und $p^{2k} \nmid n$. Diese Primzahl muß auch n_1 teilen. Wir haben also die Kongruenz $x_1^2 + y_1^2 \equiv 0 \pmod{p}$, die nur für $p = 2$ und $p \equiv 1 \pmod{4}$ bestehen kann.

Die Bedingung ist hinreichend: Wir zerlegen n in $n = n_1^2 n_2$ mit quadratfreiem n_2. Für $n_2 = 1$ ist $n = n_1^2 + 0^2$. Für $n_2 > 1$ kann n_2 höchstens die 2 und Primzahlen $p \equiv 1 \pmod{4}$ enthalten. Es ist $2 = 1^2 + 1^2$, und nach Satz 6.3 läßt sich jede dieser Primzahlen als Summe von zwei Quadraten darstellen. Besitzen nun zwei Zahlen h_1, h_2 Darstellungen $h_1 = a^2 + b^2$, $h_2 = c^2 + d^2$, so auch ihr Produkt, wie man aus

$$h_1 h_2 = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

erkennt. Insgesamt besitzt also n_2 gleichfalls eine Darstellung $n_2 = u^2 + v^2$. Dann ist auch $n = (n_1 u)^2 + (n_1 v)^2$.

6.1.3. Gitterpunkte auf Hyperbeln

Ist in der Hyperbelgleichung $x^2 - Dy^2 = N$ die Zahl D ein vollständiges Quadrat, so ist die Bestimmung der Gitterpunkte auf der Hyperbel ganz einfach. Wir können sogar o. B. d. A. $D = 1$, $N > 0$ annehmen. In $x^2 - y^2 = N$ setzen wir $x - y = t$ und

$x + y = d$. Dann haben wir die Gleichung $t \cdot d = N$ zu lösen und wegen $x = \frac{d+t}{2}$, $y = \frac{d-t}{2}$ die Lösungen mit $t \equiv d$ (2) zu berücksichtigen. Ist $N \equiv 1$ (2), so gibt es genau $d(N)$ positive Lösungen t. Für $N \equiv 2$ (4) gibt es unter der Nebenbedingung keine Lösung. Und für $N \equiv 0$ (4) finden wir $d\left(\frac{N}{4}\right)$ positive Lösungen t. Da mit t, d auch $-t, -d$ eine Lösung ist, haben wir den Satz:

Satz 6.6. *Die Anzahl der Gitterpunkte auf der Hyperbel $x^2 - y^2 = N$ beträgt $2d(N)$ für $N \equiv 1$ (2), 0 für $N \equiv 2$ (4), $2d\left(\frac{N}{4}\right)$ für $N \equiv 0$ (4).*

Von jetzt an sei stets D kein vollständiges Quadrat, das heißt, $\sqrt{D}$ ist irrational. Wir beginnen mit den Hyperbeln $x^2 - Dy^2 = \pm 1$.

Hilfssatz 6.1. *Ist D kein vollständiges Quadrat, dann hat die Ungleichung*

$$|x^2 - Dy^2| < 1 + 2\sqrt{D}$$

unendlich viele Lösungen in natürlichen Zahlen x, y.

Beweis. Die Ungleichung $\left|\frac{x}{y} - \sqrt{D}\right| < \frac{1}{y^2}$ hat unendlich viele Lösungen, denn sie wird wenigstens von den sämtlichen Näherungsbrüchen der Kettenbruchentwicklung von $\sqrt{D}$ erfüllt. Dann ist

$$\left|\frac{x}{y} + \sqrt{D}\right| = \left|\left(\frac{x}{y} - \sqrt{D}\right) + 2\sqrt{D}\right| < \frac{1}{y^2} + 2\sqrt{D},$$

$$|x^2 - Dy^2| = \left|x - y\sqrt{D}\right| \left|x + y\sqrt{D}\right| < \frac{1}{y^2} + 2\sqrt{D} \leqq 1 + 2\sqrt{D}.$$

Satz 6.7. *Ist D kein vollständiges Quadrat, dann liegt auf der Hyperbel $x^2 - Dy^2 = 1$ wenigstens ein Gitterpunkt mit $y \neq 0$.*

Beweis. Nach Hilfssatz 6.1 gibt es wenigstens eine ganze Zahl $k \neq 0$, für die die Gleichung $x^2 - Dy^2 = k$ unendlich viele Lösungen hat. Es bezeichne L die Menge aller Lösungen (x, y). Wir betrachten die Zahlen x, y modulo $|k|$. Wie früher bezeichne $\bar{z}$ die Restklasse modulo $|k|$, in der z liegt. Durchläuft (x, y) die Menge L, so erhält man höchstens k^2 verschiedene Paare $(\bar{x}, \bar{y})$. Dadurch erhalten wir eine Zerlegung von L in Klassen, indem wir (x_1, y_1), (x_2, y_2) in dieselbe Klasse tun, wenn $\bar{x}_1 = \bar{x}_2$ und $\bar{y}_1 = \bar{y}_2$ sind. Da L unendlich viele Elemente enthält und es nur endlich viele Paare $(\bar{x}, \bar{y})$ gibt, besitzt wenigstens eine der Klassen unendlich viele Elemente. In einer solchen Klasse gibt es daher mindestens zwei Paare (x_1, y_1), (x_2, y_2) mit $|x_1| \neq |x_2|$, $|y_1| \neq |y_2|$.

Aus $x_1 \equiv x_2 \quad (|k|)$, $y_1 \equiv y_2 \quad (|k|)$ folgt

$$x_1x_2 - Dy_1y_2 \equiv x_1^2 - Dy_1^2 \equiv 0 \quad (|k|),$$
$$x_1y_2 - x_2y_1 \equiv 0 \quad (|k|).$$

Setzen wir

$$x_1x_2 - Dy_1y_2 = ku, \qquad x_1y_2 - x_2y_1 = kv,$$

so ist

$$\begin{aligned}(x_1 - y_1\sqrt{D})(x_2 + y_2\sqrt{D}) &= k\ (u + v\sqrt{D}),\\ (x_1 + y_1\sqrt{D})(x_2 - y_2\sqrt{D}) &= h\ (u - v\sqrt{D}).\end{aligned}$$

Durch Multiplikation beider Gleichungen erhalten wir

$$k^2 = (x_1^2 - Dy_1^2)(x_2^2 - Dy_2^2) = k^2(u^2 - Dv^2)$$

und $u^2 - Dv^2 = 1$. Der Satz wird bewiesen sein, wenn wir noch zeigen können, daß für die erhaltene Lösung (u, v) gilt $v \neq 0$. Wäre nämlich $v = 0$, so müßte $u = \pm 1$ sein. Es folgt dann

$$(x_1 - y_1\sqrt{D})(x_2 + y_2\sqrt{D})(x_2 - y_2\sqrt{D}) = \pm k(x_2 - y_2\sqrt{D}).$$

Andererseits ist aber

$$(x_1 - y_1\sqrt{D})(x_2 + y_2\sqrt{D})(x_2 - y_2\sqrt{D}) = k(x_1 - y_1\sqrt{D}).$$

Hieraus erhalten wir $|x_1| = |x_2|$, $|y_1| = |y_2|$ im Widerspruch zur Ausgangssituation.

Mit diesem Satz ist die Existenz einer nicht-trivialen Lösung gesichert. Darüber hinaus soll jetzt das Vorhandensein unendlich vieler Lösungen nachgewiesen werden. Dazu verabreden wir folgendes:

Definition 6.1. Erfüllen die ganzen Zahlen x, y die Gleichung $x^2 - Dy^2 = N$ (D kein vollständiges Quadrat, $N \gtrless 0$), so heiße $x + y\sqrt{D}$ eine *Lösung*. Die kleinste Lösung $x_1 + y_1\sqrt{D}$ mit $x_1, y_1 > 0$ heiße *Fundamentallösung*.

Satz 6.8. *Ist D kein vollständiges Quadrat, dann liegen auf der Hyperbel $x^2 - Dy^2 = 1$ unendlich viele Gitterpunkte. Ist $x_1 + y_1\sqrt{D}$ die Fundamentallösung, so sind die sämtlichen Lösungen $x_n + y_n\sqrt{D}$ mit $x_n, y_n > 0$ gegeben durch*

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n \qquad (n = 1, 2, \ldots).$$

Beweis. Nach Satz 6.7 liegt auf der Hyperbel wenigstens ein nicht-trivialer Gitterpunkt, so daß die Fundamentallösung existiert. Die angegebenen Werte $x_n + y_n\sqrt{D}$ bilden im Sinne der Definition wegen

$$x_n^2 - Dy_n^2 = (x_1^2 - Dy_1^2)^n = 1$$

tatsächlich Lösungen. Nehmen wir an, es gibt noch eine weitere Lösung $u + v\sqrt{D}$ mit $u, v > 0$. Hierzu finden wir ein n mit

$$\begin{aligned}(x_1 + y_1\sqrt{D})^n < u + v\sqrt{D} &< (x_1 + y_1\sqrt{D})^{n+1},\\ x_n + y_n\sqrt{D} < u + v\sqrt{D} &< (x_n + y_n\sqrt{D})(x_1 + y_1\sqrt{D}).\end{aligned}$$

Da $x_n - y_n\sqrt{D} > 0$ ist, finden wir hieraus

$$1 < (u + v\sqrt{D})(x_n - y_n\sqrt{D}) < x_1 + y_1\sqrt{D}. \tag{6}$$

Setzen wir

$$(u + v\sqrt{D})(x_n - y_n\sqrt{D}) = x + y\sqrt{D},$$

so erhalten wir eine weitere Lösung $x + y\sqrt{D}$, denn es ist

$$x^2 - Dy^2 = (u^2 - Dv^2)(x_n^2 - Dy_n^2) = 1.$$

Aus

$$(u - v\sqrt{D})(x_n + y_n\sqrt{D}) = x - y\sqrt{D}$$

und $u > v\sqrt{D}$ ergibt sich $x > y\sqrt{D}$. Daher ist

$$0 < x - y\sqrt{D} = \frac{1}{x + y\sqrt{D}} < 1,$$

und das bedeutet $x > 0$ und $y > 0$. Nach (6) ist

$$x + y\sqrt{D} < x_1 + y_1\sqrt{D},$$

was im Widerspruch zur Eigenschaft von $x_1 + y_1\sqrt{D}$ als Fundamentallösung steht.

Nach diesem Satz besteht also für die Angabe von Lösungen das Problem darin, wenigstens eine Lösung zu finden. Das kann geschehen, indem man in $x^2 = 1 + Dy^2$ nacheinander für y die Werte 1, 2, ... einsetzt und nachsieht, ob sich für $1 + Dy^2$ ein vollständiges Quadrat ergibt. So ist beispielsweise für die Gleichung $x^2 - 5y^2 = 1$ die Fundamentallösung durch $9 + 4\sqrt{5}$ gegeben. Es gibt auch ein systematisches Verfahren, welches die Kettenbruchentwicklung von $\sqrt{D}$ ausnutzt. Jedoch soll darauf nicht eingegangen werden.

Wenden wir uns jetzt der Gleichung $x^2 - Dy^2 = -1$ zu.

Satz 6.9. *Ist D kein vollständiges Quadrat, dann liegen auf der Hyperbel $x^2 - Dy^2 = -1$ entweder keine oder unendlich viele Gitterpunkte. Ist im zweiten Fall $\xi_1 + \eta_1\sqrt{D}$ die Fundamentallösung, so sind die sämtlichen Lösungen $\xi_n + \eta_n\sqrt{D}$ mit $\xi_n, \eta_n > 0$ durch*

$$\xi_n + \eta_n\sqrt{D} = (\xi_1 + \eta_1\sqrt{D})^{2n-1} \qquad (n = 1, 2, \ldots)$$

gegeben. Ferner liefert

$$x + y\sqrt{D} = (\xi_1 + \eta_1\sqrt{D})^2$$

die Fundamentallösung von $x^2 - Dy^2 = 1$.

Beweis. Wir führen den Beweis in drei Schritten.

1. Die Werte $\xi_n + \eta_n\sqrt{D}$ sind im Fall der Lösbarkeit Lösungen, da

$$\xi_n^2 - D\eta_n^2 = (\xi_1^2 - D\eta_1^2)^{2n-1} = -1.$$

2. Ebenso ist $x + y\sqrt{D} = \left(\xi_1 + \eta_1\sqrt{D}\right)^2$ wegen

$$x^2 - Dy^2 = (\xi_1^2 - D\eta_1^2)^2 = 1$$

Lösung der Gleichung $x^2 - Dy^2 = 1$. Nehmen wir an, $\left(\xi_1 + \eta_1\sqrt{D}\right)^2$ ist nicht Fundamentallösung, so muß

$$1 < x_1 + y_1\sqrt{D} < \left(\xi_1 + \eta_1\sqrt{D}\right)^2$$

gelten, wenn $x_1 + y_1\sqrt{D}$ die Fundamentallösung von $x^2 - Dy^2 = 1$ ist. Es ist $0 < -\xi_1 + \eta_1\sqrt{D} < 1$ wegen

$$\left(-\xi_1 + \eta_1\sqrt{D}\right)\left(\xi_1 + \eta_1\sqrt{D}\right) = -\xi_1^2 + D\eta_1^2 = 1$$

und daher

$$-\xi_1 + \eta_1\sqrt{D} < \left(-\xi_1 + \eta_1\sqrt{D}\right)\left(x_1 + y_1\sqrt{D}\right) < \xi_1 + \eta_1\sqrt{D}\,.$$

Setzen wir jetzt

$$\left(-\xi_1 + \eta_1\sqrt{D}\right)\left(x_1 + y_1\sqrt{D}\right) = \xi_0 + \eta_0\sqrt{D}\,,$$

so erkennen wir

$$(\xi_1^2 - D\eta_1^2)\,(x_1^2 - Dy_1^2) = \xi_0^2 - D\eta_0^2 = -1$$

und

$$-\xi_1 + \eta_1\sqrt{D} < \xi_0 + \eta_0\sqrt{D} < \xi_1 + \eta_1\sqrt{D}\,.$$

Wir führen jetzt den Widerspruch herbei, indem wir alle möglichen Vorzeichenkombinationen von ξ_0, η_0 ausschließen. $\xi_0 = 0$ oder $\eta_0 = 0$ kann sowieso nicht sein.

a) $\xi_0 > 0$ und $\eta_0 > 0$ ist unmöglich, da $\xi_0 + \eta_0\sqrt{D} < \xi_1 + \eta_1\sqrt{D}$ und $\xi_1 + \eta_1\sqrt{D}$ Fundamentallösung ist.

b) $\xi_0 < 0$ und $\eta_0 > 0$ ist unmöglich, da sich aus $-\xi_1 + \eta_1\sqrt{D} < \xi_0 + \eta_0\sqrt{D}$ die Ungleichungen

$$\frac{\left(-\xi_1 + \eta_1\sqrt{D}\right)\left(\xi_1 + \eta_1\sqrt{D}\right)}{\xi_1 + \eta_1\sqrt{D}} < \frac{\left(\xi_0 + \eta_0\sqrt{D}\right)\left(-\xi_0 + \eta_0\sqrt{D}\right)}{-\xi_0 + \eta_0\sqrt{D}},$$

$$\frac{1}{\xi_1 + \eta_1\sqrt{D}} < \frac{1}{-\xi_0 + \eta_0\sqrt{D}}$$

ergeben. Die Ungleichung $-\xi_0 + \eta_0\sqrt{D} < \xi_1 + \eta_1\sqrt{D}$ kann aber nicht bestehen, weil $\xi_1 + \eta_1\sqrt{D}$ Fundamentallösung ist.

c) $\xi_0 < 0$ und $\eta_0 < 0$ ist unmöglich wegen

$$0 < -\xi_1 + \eta_1\sqrt{D} < \xi_0 + \eta_0\sqrt{D}.$$

d) $\xi_0 > 0$ und $\eta_0 < 0$ ist unmöglich, da sich aus $\xi_0^2 - D\eta_0^2 = -1$ die Ungleichung $\xi_0 < |\eta_0|\sqrt{D}$ und daraus $\xi_0 + \eta_0\sqrt{D} < 0$ ergibt.

3. Wir nehmen an, es gibt außer den im Satz genannten Lösungen eine weitere $u + v\sqrt{D}$ mit $u, v > 0$. Dann gibt es ein n mit

$$\left(\xi_1 + \eta_1\sqrt{D}\right)^{2n-1} < u + v\sqrt{D} < \left(\xi_1 + \eta_1\sqrt{D}\right)^{2n+1}.$$

Multiplizieren wir die Ungleichung mit $\left(\xi_1 - \eta_1\sqrt{D}\right)^{2n}$ und setzen

$$\left(\xi_1 - \eta_1\sqrt{D}\right)^{2n}\left(u + v\sqrt{D}\right) = x + y\sqrt{D},$$

so ist $x^2 - Dy^2 = -1$ und

$$0 < \frac{1}{\xi_1 + \eta_1\sqrt{D}} < x + y\sqrt{D} < \xi_1 + \eta_1\sqrt{D}.$$

Genau wie im zweiten Teil des Beweises schließen wir alle Vorzeichenkombinationen von x, y aus und erzielen den gewünschten Widerspruch.

a) $x > 0$ und $y > 0$ ist unmöglich, da $x + y\sqrt{D} < \xi_1 + \eta_1\sqrt{D}$ und $\xi_1 + \eta_1\sqrt{D}$ Fundamentallösung ist.

b) $x < 0$ und $y > 0$ ist unmöglich, da

$$\frac{1}{x + y\sqrt{D}} = -x + y\sqrt{D} < \xi_1 + \eta_1\sqrt{D}.$$

c) $x < 0$ und $y < 0$ ist wegen $0 < x + y\sqrt{D}$ unmöglich.

d) $x > 0$ und $y < 0$ ist unmöglich, da aus $x^2 < Dy^2$ folgt $x + y\sqrt{D} < 0$.

In diesem Satz haben wir insbesondere von der Fundamentallösung der Gleichung $x^2 - Dy^2 = -1$ auf die von $x^2 - Dy^2 = 1$ geschlossen. Aber auch die Umkehrung ist möglich.

Satz 6.10. *Ist* $x_1 + y_1\sqrt{D}$ *die Fundamentallösung von* $x^2 - Dy^2 = 1$, *so bildet*

$$\sqrt{\frac{x_1 - 1}{2}} + \sqrt{\frac{x_1 + 1}{2D}}\sqrt{D}$$

die Fundamentallösung von $x^2 - Dy^2 = -1$, *sofern* $\sqrt{\frac{x_1 - 1}{2}}, \sqrt{\frac{x_1 + 1}{2D}}$ *natürliche Zahlen sind; andernfalls ist die Gleichung* $x^2 - Dy^2 = -1$ *unlösbar.*

Beweis. Ist $\xi_1 + \eta_1\sqrt{D}$ die Fundamentallösung von $x^2 - Dy^2 = -1$, so ist nach Satz 6.9

$$x_1 + y_1\sqrt{D} = \left(\xi_1 + \eta_1\sqrt{D}\right)^2$$

die Fundamentallösung von $x^2 - Dy^2 = 1$. Aus dieser Gleichung folgt für ξ_1, η_1 das Gleichungssystem

$$x_1 = \xi_1^2 + D\eta_1^2, \qquad y_1 = 2\xi_1\eta_1.$$

Durch Einsetzen der zweiten Gleichung in die erste erhalten wir

$$x_1 = \xi_1^2 + \frac{Dy_1^2}{4\xi_1^2}, \qquad (2\xi_1^2 - x_1)^2 = x_1^2 - Dy_1^2 = 1.$$

Also ist

$$\xi_1 = \sqrt{\frac{x_1 \pm 1}{2}} \qquad \text{und} \qquad \eta_1 = \frac{y_1}{2\sqrt{\frac{x_1 \pm 1}{2}}} = \sqrt{\frac{x_1 \mp 1}{2D}}.$$

Wegen

$$\xi_1^2 - D\eta_1^2 = \frac{x_1 \pm 1}{2} - \frac{x_1 \mp 1}{2} = -1$$

kann in der Darstellung von ξ_1, η_1 nur das untere Vorzeichen gelten.

Beispiel. Aus der Fundamentallösung $9 + 4\sqrt{5}$ von $x^2 - 5y^2 = 1$ erhält man die Fundamentallösung $2 + \sqrt{5}$ von $x^2 - 5y^2 = -1$.

Wie der folgende Satz zeigt, ist dieses Beispiel verallgemeinerungsfähig.

Satz 6.11. *Es sei p eine Primzahl mit $p \equiv 1$ (4). Dann liegen auf der Hyperbel $x^2 - py^2 = -1$ unendlich viele Gitterpunkte.*

Beweis. $x_1 + y_1\sqrt{p}$ sei Fundamentallösung von $x^2 - py^2 = 1$. Wäre $x_1 \equiv 0$ (2), so wäre $py_1^2 \equiv -1$ (4), was nicht sein kann. Dann ist also $x_1 \equiv 1$ (2) und $(x_1 - 1, x_1 + 1) = 2$. Daher folgt aus

$$(x_1 - 1)(x_1 + 1) = x_1^2 - 1 = py_1^2$$

mit positiven Zahlen a, b

$$x_1 \pm 1 = 2a^2, \qquad x_1 \mp 1 = 2pb^2$$

und $a^2 - pb^2 = \pm 1$. Aus

$$4pa^2b^2 = x_1^2 - 1 = py_1^2$$

ergibt sich $a < x_1$ und $b < y_1$. Da $x_1 + y_1\sqrt{D}$ Fundamentallösung von $x^2 - py^2 = 1$ ist, kann nur $a^2 - pb^2 = -1$ sein. Das heißt, nur das untere Vorzeichen ist zutreffend. Die Behauptung resultiert nun aus $x_1 - 1 = 2a^2$, $x_1 + 1 = 2pb^2$ in Anwendung des Satzes 6.10.

Die Behandlung der allgemeinen Hyperbeln $x^2 - Dy^2 = N$ mit positivem oder negativem N stützt sich auf die Ergebnisse, die wir für $N = 1$ erzielt haben. Zunächst stellen wir fest, daß mit einer Lösung $x + y\sqrt{D}$ von $x^2 - Dy^2 = N$ und einer Lösung $\xi + \eta\sqrt{D}$ von $\xi^2 - D\eta^2 = 1$ auch

$$\left(x + y\sqrt{D}\right)\left(\xi + \eta\sqrt{D}\right) = x\xi + Dy\eta + (x\eta + y\xi)\sqrt{D}$$

eine Lösung von $x^2 - Dy^2 = N$ ist. Wir nennen sie eine zu $x + y\sqrt{D}$ assoziierte Lösung. Man stellt unschwer fest, daß die Assoziiertheit eine Äquivalenzrelation in der Menge aller Lösungen $x + y\sqrt{D}$ darstellt. Damit bilden die sämtlichen zu $x + y\sqrt{D}$ assoziierten Lösungen eine Äquivalenzklasse $K = K(x, y)$, die nach Satz 6.8 unendlich viele Elemente enthält.

Ist $x' + y'\sqrt{D} \in K(x, y)$, so besteht eine Darstellung

$$x' + y'\sqrt{D} = (x + y\sqrt{D})(\xi + \eta\sqrt{D}).$$

Hieraus finden wir

$$\begin{aligned} xx' - Dyy' + (xy' - x'y)\sqrt{D} &= (x' + y'\sqrt{D})(x - y\sqrt{D}) \\ &= (x^2 - Dy^2)(\xi + \eta\sqrt{D}) \\ &= N(\xi + \eta\sqrt{D}). \end{aligned}$$

Daher sind

$$\begin{aligned} xx' - Dyy' &\equiv 0 \quad (|N|), \\ xy' - x'y &\equiv 0 \quad (|N|) \end{aligned}$$

notwendige Bedingungen, daß $x + y\sqrt{D}$ und $x' + y'\sqrt{D}$ zur selben Klasse gehören. Sie sind aber auch hinreichend. Denn sind $x + y\sqrt{D}$ und $x' + y'\sqrt{D}$ Lösungen mit dieser Eigenschaft, so definieren wir

$$\xi := \frac{xx' - Dyy'}{N}, \qquad \eta := \frac{xy' - x'y}{N},$$

und es ist

$$\xi^2 - D\eta^2 = \frac{1}{N^2}(x^2 - Dy^2)(x'^2 - Dy'^2) = 1.$$

Es bezeichne noch $\bar{K}$ die zu K konjugierte Klasse, indem bei den Elementen von K die Zahl $\sqrt{D}$ durch $-\sqrt{D}$ ersetzt wird. Wir benutzen die Definition 6.1 in leicht abgewandelter Form: $u + v\sqrt{D}$ heiße *Fundamentallösung der Klasse* K, wenn v der kleinstmögliche nichtnegative Wert ist. Für $K \neq \bar{K}$ ist u eindeutig bestimmt, denn $-u + v\sqrt{D} \in \bar{K}$. Ist dagegen $K = \bar{K}$, so werde $u \geqq 0$ gefordert.

Satz 6.12. *Ist $u + v\sqrt{D}$ die Fundamentallösung der Klasse K der Gleichung $u^2 - Dv^2 = N > 0$, und ist $x_1 + y_1\sqrt{D}$ die Fundamentallösung der Gleichung $x^2 - Dy^2 = 1$, so gilt*

$$0 \leqq v \leqq \frac{y_1}{\sqrt{2(x_1 + 1)}}\sqrt{N}, \tag{7}$$

$$0 < |u| \leqq \sqrt{\frac{1}{2}(x_1 + 1)N}. \tag{8}$$

Folgerung. *Es gibt nur endlich viele Lösungsklassen. Gibt es keine u und v mit* $u^2 - Dv^2 = N$, *die den Ungleichungen* (7), (8) *genügen, so ist diese Gleichung unlösbar.*

Beweis. Für $N > 0$ ist $u \neq 0$. Wir können ohne Beschränkung der Allgemeinheit für K diejenige Klasse wählen, für die $u > 0$ ist. Mit der Fundamentallösung $u + v\sqrt{D} \in K$ ist

$$\left(u + v\sqrt{D}\right)\left(x_1 - y_1\sqrt{D}\right) = ux_1 - Dvy_1 + (x_1 v - y_1 u)\sqrt{D}$$

ein Element von K. Weil

$$ux_1 - Dvy_1 = ux_1 - \sqrt{(u^2 - N)(x_1^2 - 1)} > 0$$

ist, muß sogar $ux_1 - Dvy_1 \geqq u$ sein. Daraus ergibt sich

$$u^2(x_1 - 1)^2 \geqq D^2 v^2 y_1^2 = (u^2 - N)(x_1^2 - 1),$$

$$u^2 \leqq \frac{1}{2}(x_1 + 1)N,$$

und es folgt (8). Die Ungleichung (7) ergibt sich aus

$$v^2 = \frac{u^2 - N}{D} \leqq \frac{x_1 - 1}{2D} N = \frac{x_1^2 - 1}{2(x_1 + 1)\,D} N = \frac{y_1^2}{2(x_1 + 1)} N.$$

Beispiel. $u^2 - 2v^2 = 119$.
Die Fundamentallösung von $x^2 - 2y^2 = 1$ ist $3 + 2\sqrt{2}$. Nach (7) kommen für v Werte mit $0 \leqq v \leqq \frac{2}{\sqrt{8}}\sqrt{119} < 8$ in Betracht. Daraus resultieren die Lösungen $\pm 11 + \sqrt{2}$, $\pm 13 + 5\sqrt{2}$. Man überprüft leicht, daß alle vier Lösungen verschiedenen Klassen angehören. Also gibt es vier Lösungsklassen mit den genannten Fundamentallösungen.

Satz 6.13. *Ist* $u + v\sqrt{D}$ *die Fundamentallösung der Klasse K der Gleichung* $u^2 - Dv^2 = -N < 0$, *und ist* $x_1 + y_1\sqrt{D}$ *die Fundamentallösung der Gleichung* $x^2 - Dy^2 = 1$, *so gilt*

$$0 < v \leqq \frac{y_1}{\sqrt{2(x_1 - 1)}}\sqrt{N}, \tag{9}$$

$$0 \leqq |u| \leqq \sqrt{\frac{1}{2}(x_1 - 1)N}. \tag{10}$$

Folgerung *Es gibt nur endlich viele Lösungsklassen. Gibt es keine u und v mit* $u^2 - Dv^2 = -N$, *die den Ungleichungen* (9), (10) *genügen, so ist diese Gleichung unlösbar.*

Beweis. Ohne Beschränkung der Allgemeinheit sei $u \geqq 0$ angenommen. Mit der Fundamentallösung $u + v\sqrt{D} \in K$ ist auch

$$\left(u + v\sqrt{D}\right)\left(x_1 - y_1\sqrt{D}\right) = ux_1 - Dvy_1 + (x_1v - y_1u)\sqrt{D} \in K.$$

Wegen

$$x_1^2v^2 = \left(y_1^2 + \frac{1}{D}\right)(u^2 + N) > y_1^2u^2$$

ist $x_1v - y_1u > 0$ und wegen der Eigenschaft der Fundamentallösung $x_1v - y_1u \geqq v$. Daraus ergibt sich

$$Dv^2(x_1 - 1)^2 \geqq Dy_1^2u^2,$$
$$(u^2 + N)(x_1 - 1)^2 \geqq (x_1^2 - 1)u^2,$$
$$u^2 \leqq \frac{1}{2}(x_1 - 1)N$$

und damit (10). Die Ungleichung (9) folgt aus

$$v^2 = \frac{u^2 + N}{D} \leqq \frac{x_1 + 1}{2D}N = \frac{x_1^2 - 1}{2(x_1 - 1)D}N = \frac{y_1^2}{2(x_1 - 1)}N.$$

Beispiele.

1. $u^2 - 6v^2 = -2$.

Die Fundamentallösung von $x^2 - 6y^2 = 1$ ist $5 + 2\sqrt{6}$. Nach (9) kommt für v nur $0 < v \leqq \frac{2}{\sqrt{8}}\sqrt{2}$, also $v = 1$ in Frage. Man erhält die beiden Lösungen $\pm 2 + \sqrt{6}$. Wie man leicht feststellt, gehören sie aber zur selben Klasse. Also gibt es nur eine Lösungsklasse mit der Fundamentallösung $2 + \sqrt{6}$.

2. $u^2 - 5v^2 = -2$.

Die Fundamentallösung von $x^2 - 5y^2 = 1$ ist $9 + 4\sqrt{5}$. Aus (9) ergibt sich für v nur die Möglichkeit $v = 1$. Da $u^2 \neq 3$ ist, besitzt diese Gleichung keine Lösungen.

6.2. Darstellungen natürlicher Zahlen als Summe von Quadraten

Den Satz 6.5 kann man so formulieren: Eine natürliche Zahl $n > 1$ ist genau dann als Summe von zwei Quadraten ganzer Zahlen darstellbar, wenn jeder Primfaktor von n der Gestalt $4m + 3$ in der kanonischen Zerlegung von n einen geraden Exponenten besitzt. Also läßt sich nicht jede natürliche Zahl als Summe von zwei Quadraten darstellen. Es gibt auch unendlich viele natürliche Zahlen, die sich nicht als Summe von drei Quadraten darstellen lassen.

Satz 6.14. *Die natürlichen Zahlen* $n = 4^a(8b + 7)$, $a \geqq 0$, $b \geqq 0$, *lassen sich nicht als Summe von drei Quadraten darstellen.*

Beweis. Wir führen den Beweis durch vollständige Induktion nach a und beginnen mit $a = 0$. Es ist

$$x^2 \equiv 0 \ (8) \quad \text{für} \quad x \equiv 0 \ (4),$$
$$x^2 \equiv 4 \ (8) \quad \text{für} \quad x \equiv 2 \ (4),$$
$$x^2 \equiv 1 \ (8) \quad \text{für} \quad x \equiv 1 \ (2).$$

Nun ist stets

$$x_1^2 + x_2^2 + x_3^2 \not\equiv 7 \ (8),$$

während $8b + 7 \equiv 7 \ (8)$ ist. Nehmen wir jetzt an, $4^a(8b + 7)$ ist nicht als Summe von drei Quadraten darstellbar. Wir haben zu zeigen, daß dann auch $4^{a+1}(8b + 7)$ nicht darstellbar ist. Sei im Gegensatz dazu die Darstellung

$$4^{a+1}(8b + 7) = x_1^2 + x_2^2 + x_3^2$$

angenommen. Aus $x_1^2 + x_2^2 + x_3^2 \equiv 0 \ (4)$ folgt $x_1 \equiv x_2 \equiv x_3 \equiv 0 \ (2)$. Dann hätten wir im Widerspruch zur Induktionsannahme

$$4^a(8b + 7) = \left(\frac{x_1}{2}\right)^2 + \left(\frac{x_2}{2}\right)^2 + \left(\frac{x_3}{2}\right)^2.$$

Es ist bemerkenswert, daß sich alle Zahlen, die nicht von der Form $4^a(8b + 7)$ sind, als Summe von drei Quadraten darstellen lassen. Wegen der außerordentlichen Schwierigkeit wollen wir einen Beweis dieser Tatsache hier nicht geben. Im Jahre 1621 sprach C. G. Bachet (1581—1638) die Vermutung aus, daß sich jede natürliche Zahl als Summe von vier Quadraten darstellen läßt. Der erste vollständige Beweis gelang J. L. Lagrange, indem er von L. Euler entwickelte Ideen ausnutzte. Wir bereiten den Beweis durch einen Hilfssatz vor:

Hilfssatz 6.2. *Zu jeder Primzahl $p > 2$ gibt es ganze Zahlen x, y, m mit $x^2 + y^2 + 1 = mp$ und $0 < m < p$.*

Beweis. Die sämtlichen Zahlen x^2 mit $0 \leqq x \leqq \frac{p-1}{2}$ sind untereinander inkongruent modulo p. Entsprechendes gilt für die Zahlen $-y^2 - 1$ mit $0 \leqq y \leqq \frac{p-1}{2}$. Beide Zahlensysteme zusammen enthalten insgesamt $p + 1$ Zahlen. Da es aber modulo p nur p verschiedene Reste gibt, muß es zwei Zahlen x, y geben, so daß x^2 und $-y^2 - 1$ modulo p in die gleiche Restklasse fallen. Daher gibt es für diese Zahlen ein m mit $x^2 + y^2 + 1 = mp$. Wegen

$$0 < x^2 + y^2 + 1 < \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + 1 < p^2$$

ist $0 < m < p$.

Satz 6.15 (Lagrange). *Jede natürliche Zahl ist als Summe von vier Quadraten ganzer Zahlen darstellbar.*

Beweis. Lassen sich die Zahlen a, b als Summe von vier Quadraten,

$$a = x_1^2 + x_2^2 + x_3^2 + x_4^2, \qquad b = y_1^2 + y_2^2 + y_3^2 + y_4^2,$$

darstellen, so auf Grund der Eulerschen Identität auch ihr Produkt

$$\begin{aligned} a \cdot b = {} & (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ & + (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2. \end{aligned}$$

Es genügt also, den Satz für Primzahlen zu beweisen, die wir wegen $2 = 1^2 + 1^2 + 0^2 + 0^2$ gleich als ungerade annehmen können.

Es sei m die kleinste natürliche Zahl mit

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp.$$

Nach Hilfssatz 6.2 gibt es ganze Zahlen x_1, x_2, x_3, x_4, m mit dieser Eigenschaft, und es ist überdies $m < p$. Wir haben $m = 1$ zu zeigen und unterscheiden zwei Fälle.

1. Es sei $m \equiv 0 \pmod 2$. Für die x_i ergeben sich drei Möglichkeiten. Entweder sind alle x_i gerade oder alle ungerade oder zwei (etwa x_1, x_2) gerade und zwei (nunmehr x_3, x_4) ungerade. In jedem Fall sind die Zahlen $\frac{x_1 \pm x_2}{2}, \frac{x_3 \pm x_4}{2}$ ganz. Dann widerspricht aber die Gleichung

$$\left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2 = \frac{m}{2}\,p$$

der Minimumeigenschaft von m.

2. Es sei $m \equiv 1 \pmod 2$, $m \geqq 3$. Zu jedem x_k wird ein y_k bestimmt mit

$$y_k \equiv x_k \pmod m, \qquad |y_k| < \frac{m}{2} \qquad (k = 1, 2, 3, 4).$$

Dann ist

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod m,$$

und es gibt eine ganze Zahl r mit

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = mr.$$

Es muß $r > 0$ sein. Denn wäre $r = 0$, so würde $y_1 = y_2 = y_3 = y_4 = 0$ und m ein Teiler aller x_k sein. Das zieht aber $m^2 \mid mp$ nach sich, was wegen $m < p$ nicht möglich sein kann. Wegen $|y_k| < \frac{m}{2}$ für alle k ist

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 < m^2$$

und daher $r < m$.

Die Zahlen mr und mp sind beide durch vier Quadrate darstellbar, und auf Grund der Eulerschen Identität ist

$$mr \cdot mp = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

mit

$$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m},$$
$$z_2 = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \equiv 0 \pmod{m},$$
$$z_3 = x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4 \equiv 0 \pmod{m},$$
$$z_4 = x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2 \equiv 0 \pmod{m}.$$

Damit ist

$$rp = \left(\frac{z_1}{m}\right)^2 + \left(\frac{z_2}{m}\right)^2 + \left(\frac{z_3}{m}\right)^2 + \left(\frac{z_4}{m}\right)^2,$$

was wegen $0 < r < m$ gegen die Minimumeigenschaft von m verstößt.

Insgesamt kann also nur $m = 1$ sein.

Wir stellen uns jetzt die schärfere Frage, wie oft eine natürliche Zahl als Summe von zwei beziehungsweise vier Quadraten darstellbar ist. Wir haben uns schon in Abschnitt 5.7.2. mit der durchschnittlichen Größenordnung von $r(n)$ beschäftigt. Jetzt geht es uns um eine genaue Bestimmung von $r(n)$ und ebenso hinsichtlich der Darstellungen von n als Summe von vier Quadraten. Wir schreiben nunmehr für $r(n) = r_2(n)$ und erklären allgemeiner:

Definition 6.2. Es bezeichne $r_k(n)$ die Anzahl der Darstellungen der natürlichen Zahl n als Summe von k ($k \geqq 2$) Quadraten ganzer Zahlen. Es sei $r_k(0) = 1$.

Der Bestimmung von $r_2(n)$ schicken wir drei Hilfssätze voraus. Der erste Hilfssatz ist eine Verallgemeinerung der Sätze 6.2 für $D = 1$ und 6.3.

Hilfssatz 6.3. *Es sei $n > 1$ und $z^2 \equiv -1 \pmod{n}$. Dann ist n eindeutig in der Form $n = x^2 + y^2$ mit $x, y > 0$, $(x, y) = 1$, $yz \equiv x \pmod{n}$ darstellbar.*

Beweis. Nach Satz 4.7 gibt es zu $\frac{z}{n}$ und $\sqrt{n}$ eine Zahl $\frac{a}{y}$, $(a, y) = 1$, mit $1 \leqq y \leqq \sqrt{n}$ und

$$\left|\frac{z}{n} + \frac{a}{y}\right| < \frac{1}{y\sqrt{n}}.$$

Setzt man $yz + an = x$, so ist $yz \equiv x \pmod{n}$ und $|x| < \sqrt{n}$. Für diese Zahlen x, y gilt

$$x^2 + y^2 \equiv y^2(z^2 + 1) \equiv 0 \pmod{n}.$$

Wegen $0 < x^2 + y^2 < 2n$ folgt hieraus $x^2 + y^2 = n$. Es ist auch $(x, y) = 1$, denn aus

$$n = x^2 + y^2 = (yz + an)^2 + y^2 = (z^2 + 1)\, y^2 + 2anyz + a^2n^2$$

folgt

$$1 = \left(\frac{z^2 + 1}{n}\, y + az\right) y + (yz + an)\, a = \left(\frac{z^2 + 1}{n}\, y + az\right) y + ax.$$

Und diese Gleichung kann nur für $(x, y) = 1$ bestehen. Es ist $x \neq 0$, weil sonst $y^2 = n > 1$ und daher $(x, y) > 1$ wäre. Für positives x liefern dann x, y und für negatives x die Zahlen $y, -x$ die gewünschte Darstellung von n, denn in diesem Fall ist

$$(-x)\, z \equiv -yz^2 \equiv y \quad (n).$$

Nun haben wir noch zu zeigen, daß die Darstellung von n eindeutig ist. Nehmen wir an, n besitzt die beiden Darstellungen

$$n = x^2 + y^2 = x_1^2 + y_1^2$$

entsprechend den Bedingungen des Satzes. Dann ist

$$n^2 = (x^2 + y^2)\,(x_1^2 + y_1^2) = (xx_1 + yy_1)^2 + (xy_1 - x_1y)^2$$

mit

$$xx_1 + yy_1 \equiv (z^2 + 1)\, yy_1 \equiv 0 \quad (n).$$

Daher ist

$$xx_1 + yy_1 = n, \qquad xy_1 - x_1y = 0,$$

und hieraus folgt sofort $x = x_1, y = y_1$.

Hilfssatz 6.4. *Es bezeichne $\varrho(n)$ die Anzahl der Lösungen von $z^2 \equiv -1 \quad (n)$. Dann ist die Anzahl der Darstellungen von n in der Form $n = x^2 + y^2$ mit ganzen Zahlen x, y und $(x, y) = 1$ gegeben durch $4\varrho(n)$.*

Beweis. Der Fall $n = 1$ ist trivial. Für $n > 1$ sind $x, y \neq 0$, da $(x, y) = 1$. Dann ist die Anzahl der Lösungen $n = x^2 + y^2$, $(x, y) = 1$ gleich der vierfachen Anzahl unter der Nebenbedingung $x, y > 0$. Zu jedem z mit $z^2 \equiv -1 \quad (n)$ gibt es nach Hilfssatz 6.3 genau eine solche Darstellung von n mit $yz \equiv x \quad (n)$. Umgekehrt liefert jede derartige Darstellung von n genau eine Lösung der Kongruenz $z^2 \equiv -1 \quad (n)$. Denn aus $(x, y) = 1$ folgt einerseits die eindeutige Lösbarkeit von $yz \equiv x \quad (n)$, andererseits $(y, n) = 1$ und deshalb wegen

$$x^2 + y^2 \equiv y^2(z^2 + 1) \equiv 0 \quad (n)$$

schließlich $z^2 \equiv -1 \quad (n)$.

Hilfssatz 6.5. $r_2(n) = 4 \sum_{t^2 \mid n} \varrho\left(\frac{n}{t^2}\right)$.

Beweis. Ist in der Darstellung $n = x^2 + y^2$ der größte gemeinsame Teiler $(x, y) = t$, so setzen wir $x = x_1 t$, $y = y_1 t$ und erhalten

$$\frac{n}{t^2} = x_1^2 + y_1^2, \qquad (x_1, y_1) = 1.$$

Durchläuft t alle natürlichen Zahlen mit $t^2 \mid n$, so ergibt sich aus Hilfssatz 6.4 die Behauptung.

Satz 6.16 (Gauss). *Es bezeichne*

$$\chi(n) = \begin{cases} 0 & \text{für } n \equiv 0 \quad (2) \\ (-1)^{\frac{n-1}{2}} & \text{für } n \equiv 1 \quad (2) \end{cases}$$

und $\delta(n) = 1 * \chi(n)$, *also*

$$\delta(n) = \sum_{\substack{t \mid n \\ t \equiv 1 \ (4)}} 1 - \sum_{\substack{t \mid n \\ t \equiv 3 \ (4)}} 1 .$$

Dann ist

$$r_2(n) = 4\delta(n) .$$

Beweis. Für $n = 1$ ist alles klar. Wir vermerken, daß $\chi(n)$ als Restklassencharakter multiplikativ ist und daher auch $\delta(n)$. Aber auch $\varrho(n)$ ist nach Satz 2.10 multiplikativ und nach Hilfssatz 6.5 dann auch $\frac{1}{4} r_2(n)$. Daher genügt es, die Behauptung für Primzahlpotenzen zu beweisen. Wir unterscheiden die Fälle $p = 2$, $p \equiv 1 \ (4)$, $p \equiv 3 \ (4)$.

Für $p = 2$ ist

$$\varrho(2^\nu) = \begin{cases} 1 & \text{für } \nu = 1, \\ 0 & \text{für } \nu > 1. \end{cases}$$

Damit ist nach Hilfssatz 6.5 und der Definition von $\delta(n)$

$$r_2(2^\nu) = 4\delta(2^\nu) .$$

Für $p \equiv 1 \ (4)$ ist $\varrho(p^\nu) = 2$ für $\nu > 0$ und

$$r_2(p^\nu) = 4(\nu + 1) = 4\delta(p^\nu) .$$

Für $p \equiv 3 \ (4)$ ist $\varrho(p^\nu) = 0$ für $\nu > 0$ und

$$r_2(p^\nu) = \begin{cases} 4 & \text{für } \nu \equiv 0 \quad (2), \\ 0 & \text{für } \nu \equiv 1 \quad (2) \end{cases}$$
$$= 4\delta(p^\nu) .$$

Dieses Ergebnis wurde von C. G. J. Jacobi (1804—1851) unter Benutzung der Theorie der elliptischen Funktionen erneut bewiesen. Diese Methode war wirksam genug, um auch $r_k(n)$ für $k > 2$ zu behandeln. Es soll jetzt das Ergebnis für $k = 4$ dargestellt werden, allerdings nach einer später gefundenen elementaren Methode von E. Landau. Wir bereiten den Satz wieder durch zwei Hilfssätze vor.

Hilfssatz 6.6. *Es seien* u, u_1, u_2, u_3, u_4 *positive ungerade Zahlen,* $s(u)$ *bezeichne die Anzahl der Lösungen von*

$$4u = u_1^2 + u_2^2 + u_3^2 + u_4^2 .$$

Dann ist $s(u) = \sigma(u)$.

Beweis. Da $u_1^2 + u_2^2 \equiv u_3^2 + u_4^2 \equiv 2 \pmod 4$ ist, setze man mit ungeraden Zahlen m, n

$$2m = u_1^2 + u_2^2, \qquad 2n = u_3^2 + u_4^2, \qquad m + n = 2u.$$

In den Darstellungen $2k = x^2 + y^2$ mit ungeradem k sind die x, y ebenfalls ungerade. Da die u_i $(i = 1, 2, 3, 4)$ positiv sein sollen, ist nach Satz 6.16

$$s(u) = \frac{1}{16} \sum_{\substack{m+n=2u \\ m \equiv n \equiv 1 \ (2)}} r_2(2m)\, r_2(2n) = \sum_{\substack{m+n=2u \\ m \equiv n \equiv 1 \ (2)}} \delta(2m)\, \delta(2n)$$

$$= \sum_{\substack{m+n=2u \\ m \equiv u \equiv 1 \ (2)}} \sum_{t_1 \mid 2m} \chi(t_1) \sum_{t_2 \mid 2n} \chi(t_2) = \sum_{\substack{m+n=2u \\ m \equiv u \equiv 1 \ (2)}} \sum_{t_1 \mid m} \sum_{t_2 \mid n} \chi(t_1 t_2) = \sum_{t_1 d_1 + t_2 d_2 = 2u} \chi(t_1 t_2).$$

In der letzten Summe ist über alle positiven ungeraden Zahlen t_1, t_2, d_1, d_2 mit $t_1 d_1 + t_2 d_2 = 2u$ zu summieren. Betrachten wir in dieser Summe zunächst den Teil mit $t_1 = t_2$. Hierfür ist

$$\sum_{\substack{t_1 d_1 + t_2 d_2 = 2u \\ t_1 = t_2}} \chi(t_1 t_2) = \sum_{t_1 \mid u} \sum_{d_1 + d_2 = \frac{2u}{t_1}} 1 = \sum_{t_1 \mid u} \frac{u}{t_1} = \sigma(u).$$

Zur Vollendung des Beweises ist also noch

$$\sum_{\substack{t_1 d_1 + t_2 d_2 = 2u \\ t_1 > t_2}} \chi(t_1 t_2) = 0$$

zu zeigen. Die entsprechende Summe mit $t_1 < t_2$ ist dann aus Symmetriegründen ebenfalls gleich 0. Wir ordnen jetzt die Lösungen der Gleichung $t_1 d_1 + t_2 d_2 = 2u$ paarweise an, so daß einer Lösung (t_1, t_2, d_1, d_2) eineindeutig eine Lösung (t_1', t_2', d_1', d_2') mit $\chi(t_1 t_2) + \chi(t_1' t_2') = 0$ entspricht. Das erfolgt durch die Festsetzung

$$t_1' = (n+2)\, d_1 + (n+1)\, d_2, \qquad t_2' = (n+1)\, d_1 + n d_2,$$

$$d_1' = -n t_1 + (n+1)\, t_2, \qquad d_2' = (n+1)\, t_1 - (n+2)\, t_2.$$

Dabei ist $n = \left[\frac{t_2}{t_1 - t_2}\right]$ gesetzt. Man sieht sofort, daß die Zahlen t_1', t_2', d_1', d_2' positiv und ungerade sind. Eine leichte Rechnung zeigt

$$t_1' d_1' + t_2' d_2' = t_1 d_1 + t_2 d_2 = 2u.$$

Auch $t_1' > t_2'$ ist gesichert. Die Auflösung des Gleichungssystems nach t_1, t_2, d_1, d_2 bietet keine Schwierigkeiten. Es ist

$$\left[\frac{t_2'}{t_1' - t_2'}\right] = \left[\frac{n(d_1 + d_2) + d_1}{d_1 + d_2}\right] = n,$$

$$t_1 = (n+2)\, d_1' + (n+1)\, d_2', \qquad t_2 = (n+1)\, d_1' + n d_2',$$

$$d_1 = -n t_1' + (n+1)\, t_2', \qquad d_2 = (n+1)\, t_1' - (n+2)\, t_2'.$$

Schließlich ist

$$\begin{aligned} t_1t_2 + t_1't_2' &\equiv (t_1 + t_2 - 1) + (t_1' + t_2' - 1) \quad (4) \\ &\equiv t_1 + t_2 + (2n+3)\,d_1 + (2n+1)\,d_2 - 2 \quad (4) \\ &\equiv 2n(d_1 + d_2) + (t_1 + t_2 + d_1 + d_2) + 2d_1 - 2 \equiv 0 \quad (4) \end{aligned}$$

und damit $\chi(t_1t_2) = -\chi(t_1't_2')$.

Hilfssatz 6.7. *Für ungerade Zahlen u ist $r_4(2u) = 3r_4(u)$.*

Beweis. In der Darstellung

$$2u = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

sind je zwei der x_i gerade beziehungsweise ungerade. Die Anzahl der Lösungen dieser Gleichung unter der Nebenbedingung $x_1 \equiv x_2 \equiv 0 \quad (2)$, $x_3 \equiv x_4 \equiv 1 \quad (2)$ ist also $\frac{1}{6}\, r_4(2u)$. Die Substitution

$$y_1 = \frac{x_1 + x_2}{2}, \qquad y_2 = \frac{x_1 - x_2}{2}, \qquad y_3 = \frac{x_3 + x_4}{2}, \qquad y_4 = \frac{x_3 - x_4}{2} \quad (11)$$

führt die Gleichung über in

$$u = y_1^2 + y_2^2 + y_3^2 + y_4^2,$$

deren Lösungsanzahl unter der zu betrachtenden Nebenbedingung $y_1 + y_2 \equiv 0 \quad (2)$, $y_3 + y_4 \equiv 1 \quad (2)$ ebenso $\frac{1}{6}\, r_4(2u)$ ist. Andererseits ist die Lösungsanzahl dieser Gleichung ohne Nebenbedingung $r_4(u)$ und mit Nebenbedingung $\frac{1}{2}\, r_4(u)$. Denn für $u \equiv 1 \quad (4)$ kann nur genau ein y_i, also y_3 oder y_4, ungerade sein und für $u \equiv 3 \quad (4)$ genau ein y_i, also auch y_3 oder y_4, gerade sein.

Satz 6.17 (Jacobi). *Es ist*

$$r_4(n) = 8\sigma(n) \qquad \text{für} \quad n \not\equiv 0 \quad (4),$$

$$r_4(n) = 8\sigma(n) - 32\sigma\left(\frac{n}{4}\right) \qquad \text{für} \quad n \equiv 0 \quad (4).$$

Beweis. Es ist $r_4(2n) = r_4(4n)$, denn in

$$4n = x_1^2 + x_2^2 + x_3^2 + x_4^2 \quad (12)$$

ist $x_1 \equiv x_2 \equiv x_3 \equiv x_4 \quad (2)$, und die Substitution (11) gibt

$$2n = y_1^2 + y_2^2 + y_3^2 + y_4^2.$$

Setzen wir in (12) eine ungerade Zahl $n = u$ ein, so können wir die Lösungen in zwei Klassen einteilen. Entweder sind alle x_i gerade oder alle x_i ungerade. Die Anzahl der Lösungen mit geraden x_i ist $r_4(u)$, die mit ungeraden x_i nach Hilfssatz 6.6 bei Be-

achtung der Vorzeichen $16\sigma(u)$. Daher ist

$$r_4(4u) = r_4(u) + 16\sigma(u).$$

Nach Hilfssatz 6.7 folgt nun

$$3r_4(u) = r_4(2u) = r_4(4u) = r_4(u) + 16\sigma(u)$$
$$r_4(u) = 8\sigma(u).$$

Das ist die erste Behauptung des Satzes für ungerades $n = u$. Für $n \equiv 2$ (4) ergibt sich aus Hilfssatz 6.7

$$r_4(n) = 3r_4\left(\frac{n}{2}\right) = 24\sigma\left(\frac{n}{2}\right) = 8\sigma(2)\,\sigma\left(\frac{n}{2}\right) = 8\sigma(n).$$

Damit ist die erste Behauptung des Satzes vollständig bewiesen. Für $n \equiv 0$ (4) setzen wir $n = 2^k u$ mit $k \geqq 2$, $u \equiv 1$ (2). Wegen $r_4(4n) = r_4(2n)$ ist

$$\begin{aligned} r_4(n) &= r_4(2u) = 8\sigma(2u) = 24\sigma(u) \\ &= 8\{2^{k+1} - 1 - 4(2^{k-1} - 1)\}\,\sigma(u) \\ &= 8\{\sigma(2^k) - 4\sigma(2^{k-2})\}\,\sigma(u) \\ &= 8\sigma(n) - 32\sigma\left(\frac{n}{4}\right). \end{aligned}$$

6.3. Rationale Punkte auf Kurven zweiter Ordnung

In der Ebene sei eine nicht zerfallende Kurve zweiter Ordnung mit rationalen Koeffizienten gegeben. Wir stellen die Frage, ob eine solche Kurve hinsichtlich eines kartesischen Koordinatensystems rationale Punkte, das heißt Punkte mit rationalen Koordinaten, enthält. Diese Frage werden wir vollständig beantworten können.

Satz 6.18. *Auf einer Kurve zweiter Ordnung mit rationalen Koeffizienten liegen entweder keine oder unendlich viele rationale Punkte.*

Beweis. Es sei ein rationaler Punkt auf der Kurve bekannt. Dann lege man durch diesen Punkt eine Gerade mit rationalen Koeffizienten, die die Kurve in einem weiteren Punkt schneidet. Dieser zweite Schnittpunkt ist notwendigerweise rational. Da man durch den bekannten rationalen Punkt aber gleich ein ganzes Geradenbüschel mit rationalen Koeffizienten legen kann, so erhält man mit einem Punkt sofort unendlich viele rationale Punkte.

Satz 6.19. *Auf einer Parabel mit rationalen Koeffizienten liegen stets unendlich viele rationale Punkte.*

Beweis. Die Parabel sei durch

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

mit rationalen Koeffizienten und $b^2 - 4ac = 0$ gegeben. Wir können ohne Beschränkung der Allgemeinheit $c \neq 0$ annehmen. Durch Multiplikation mit $4c$ und Einsetzen von $4ac = b^2$ erhält die Gleichung die Gestalt

$$(bx + 2cy + e)^2 + d'x + f' = 0$$

mit rationalen Koeffizienten d', f', deren Größe nicht weiter interessiert.

Die Transformation

$$x' = x, \qquad y' = bx + 2cy + e$$

führt die Parabel über in

$$y'^2 + d'x' + f' = 0.$$

Dabei wird jeder rationale Punkt auf einen rationalen Punkt und umgekehrt abgebildet. Wir können uns also auf Parabeln vom Typ

$$y^2 + ax + b = 0, \qquad a \neq 0, \tag{13}$$

beschränken. Auf dieser Parabel liegt der rationale Punkt $x = -\frac{b}{a}$, $y = 0$. Nach Satz 6.18 befinden sich dann auf ihr unendlich viele rationale Punkte.

Es bereitet keine Schwierigkeit, sämtliche rationalen Punkte von (13) zu bestimmen. Wir legen Geraden

$$y = t\left(x + \frac{b}{a}\right)$$

durch den Punkt $\left(-\frac{b}{a}, 0\right)$ mit beliebigem rationalen Parameter $t \neq 0$. Der zweite Schnittpunkt mit (13) ergibt sich aus

$$t^2\left(x + \frac{b}{a}\right)^2 + ax + b = 0$$

zu

$$x = -\frac{b}{a} - \frac{a}{t^2}, \qquad y = -\frac{a}{t}.$$

Die beiden Kurventypen *Ellipse und Hyperbel* behandeln wir gemeinsam. Es sei eine Ellipse oder Hyperbel in der allgemeinen Gestalt (1) mit rationalen Koeffizienten gegeben. Die Transformationen (4) und (5) führen diese Kurven in die Gestalt $x^2 + Dy^2 = N$ mit rationalen D, N über, wobei wieder jedem rationalen Punkt der Kurve ein rationaler Punkt der transformierten Kurve entspricht und umgekehrt. Wir können uns also auf Ellipsen und Hyperbeln dieser speziellen Form beschränken. Entsprechend dem Vorgehen in der analytischen Geometrie bezeichnen wir jetzt die inhomogenen Koordinaten mit großen Buchstaben. Wir betrachten also die Gleichung

$$X^2 + DY^2 = N. \tag{14}$$

Beim Übergang zu den homogenen Koordinaten setzen wir

$$X = \frac{x}{z}, \quad Y = \frac{y}{z}, \quad D = \frac{b}{a}, \quad N = -\frac{c}{a}$$

mit ganzen Zahlen a, b, c. Die Frage nach der Lösbarkeit der Gleichung (14) in rationalen Zahlen ist dann äquivalent der Frage nach der Lösbarkeit der Gleichung

$$ax^2 + by^2 + cz^2 = 0 \tag{15}$$

in ganzen Zahlen.

Liegt auf einer Ellipse oder Hyperbel wenigstens ein rationaler Punkt, so liegen auf ihr nach Satz 6.18 sogar unendlich viele rationale Punkte, die nach dem dort im Beweis beschriebenen Verfahren bestimmt werden können. Wir wollen es anwenden, um die sämtlichen rationalen Punkte auf dem *Einheitskreis* $X^2 + Y^2 = 1$ zu bestimmen. Ein rationaler Punkt ist durch $X = -1$, $Y = 0$ gegeben. Mit dem rationalen Parameter t legen wir durch diesen Punkt das Geradenbüschel $Y = t(X + 1)$. Die zweiten Schnittpunkte ergeben sich aus

$$X^2 - 1 + t^2(X + 1)^2 = 0$$

zu

$$X = \frac{1 - t^2}{1 + t^2}, \qquad Y = \frac{2t}{1 + t^2}.$$

Diese Punkte und $(-1, 0)$ *bilden die sämtlichen rationalen Punkte auf dem Einheitskreis.* Wir setzen $t = \frac{v}{u}$ mit $u > 0$, $(u, v) = 1$ und erhalten

$$X = \frac{u^2 - v^2}{u^2 + v^2}, \qquad Y = \frac{2uv}{u^2 + v^2}.$$

Den Punkt $(-1, 0)$ bekommen wir auch mittels dieser Formel, sofern wir nachträglich $u = 0$ zulassen. Will man schließlich noch zu ganzen Zahlen x, y, z durch $X := \frac{x}{z}$, $Y := \frac{y}{z}$ übergehen, so ist noch der größte gemeinsame Teiler $d = (u^2 - v^2, 2uv, u^2 + v^2)$ zu beachten. Offensichtlich ist $d = 1$ für $u \not\equiv v \pmod 2$ und $d = 2$ für $u \equiv v \equiv 1 \pmod 2$. Somit entspricht jedem rationalen Punkt des Einheitskreises umkehrbar eindeutig eine Lösung

$$x = \frac{u^2 - v^2}{d}, \qquad y = \frac{2uv}{d}, \qquad z = \frac{u^2 + v^2}{d}$$

der diophantischen Gleichung

$$x^2 + y^2 = z^2$$

mit $(x, y, z) = 1$. Für $d = 2$ setzen wir $u = u' + v'$, $v = u' - v'$ mit $u' \not\equiv v' \pmod 2$ und erhalten ein dem Fall $d = 1$ entsprechendes Ergebnis, indem lediglich x und y

vertauscht sind. Wir können uns also allgemein auf $d = 1$, das heißt $u \not\equiv v \pmod 2$, beschränken. Sollen nur die Lösungen in natürlichen Zahlen x, y, z angegeben werden, so verlangen wir $u > v > 0$. Zusammenfassend haben wir:

Satz 6.20. *Die Gesamtheit der ganzzahligen Lösungen der Pythagoräischen Gleichung*

$$x^2 + y^2 = z^2$$

mit $x, y, z > 0$, $(x, y, z) = 1$, $y \equiv 0 \pmod 2$ *ist gegeben durch*

$$x = u^2 - v^2, \qquad y = 2uv, \qquad z = u^2 + v^2$$

mit $u > v > 0$, $(u, v) = 1$, $u \not\equiv v \pmod 2$.

Die Lösungen im Sinne dieses Satzes nennt man auch *Pythagoräische Zahlentripel*. Einige Beispiele entnimmt man der Tabelle:

u	v	x	y	z
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25
5	2	21	20	29
5	4	9	40	41

Was bei Parabeln gar nicht vorkommen konnte, kann bei Ellipsen und Hyperbeln durchaus auftreten, daß sie nämlich gar keine rationalen Punkte enthalten. So liegt beispielsweise auf dem Kreis $X^2 + Y^2 = 3$ kein rationaler Punkt. Entsprechend (15) ist hier die Gleichung $x^2 + y^2 = 3z^2$ in ganzen Zahlen mit $(x, y, z) = 1$ zu betrachten. Da aber x und y nicht durch 3 teilbar sind, ist die Kongruenz $x^2 + y^2 \equiv 0 \pmod 3$ (3) unlösbar. Ebenso liegt auf der Hyperbel $X^2 - 2Y^2 = 3$ kein rationaler Punkt, da wir hier auf die gleiche Kongruenz geführt werden.

Zur allgemeinen Behandlung der diophantischen Gleichung (15) können wir annehmen, daß die Zahlen a, b, c sämtlich verschieden von 0, nicht alle positiv und nicht alle negativ sind. Auch können wir sie quadratfrei voraussetzen mit $(a, b, c) = 1$. Selbst die Voraussetzung $(a, b) = (b, c) = (c, a) = 1$ bedeutet keine Einschränkung. Für die Lösungen der Gleichung (15) können wir gleich $(x, y, z) = 1$ annehmen. Dann ist von selbst $(x, y) = (y, z) = (z, x) = 1$. Denn wäre beispielsweise die Primzahl p ein Teiler von (x, y), so wäre auch $p^2 \mid cz^2$. Das kann aber nicht sein wegen $(x, y, z) = 1$ und c quadratfrei. Zu einer notwendigen Bedingung für die Lösbarkeit von (15) gelangt man durch eine Betrachtung der Gleichung modulo c:

$$ax^2 + by^2 \equiv 0 \pmod c.$$

Wegen $(b, c) = (x, y) = 1$ ist $(x, c) = 1$, und es gibt ein u mit $y \equiv xu \pmod c$. Daraus folgt

$$x^2(a + bu^2) \equiv 0 \pmod c,$$
$$(bu)^2 \equiv -ab \pmod c.$$

Also ist notwendig für die Lösbarkeit, daß $-ab$ quadratischer Rest modulo c ist. Durch zyklische Vertauschung erhält man die weiteren notwendigen Bedingungen $-bc$ quadratischer Rest modulo a und $-ca$ quadratischer Rest modulo b. A. M. LEGENDRE bewies, daß diese Bedingungen auch hinreichend sind.

Satz 6.21 (LEGENDRE). *Es seien a, b, c drei ganze Zahlen, die den folgenden Bedingungen genügen: Sie sind alle verschieden von 0, nicht alle positiv, nicht alle negativ. Sie sind sämtlich quadratfrei, und es ist $(a, b) = (b, c) = (c, a) = 1$.*

Notwendige und hinreichende Bedingungen für die Lösbarkeit der diophantischen Gleichung (15) *in ganzen Zahlen x, y, z mit $x^2 + y^2 + z^2 > 0$ sind: $-bc$ ist quadratischer Rest modulo a, $-ca$ ist quadratischer Rest modulo b, $-ab$ ist quadratischer Rest modulo c.*

Beweis (vgl. [13]). Die Notwendigkeit der Bedingungen wurde bereits gezeigt. Nun weisen wir nach, daß sie auch hinreichend sind. Wir können ohne Beschränkung der Allgemeinheit $|a| \leqq |b| \leqq |c|$ und daher $|ab| \leqq |ac| \leqq |bc|$ annehmen. Wir nennen $K = |ac|$ den Index der Gleichung (15) und führen den Beweis durch Induktion nach K.

Für $K = 1$ ist $|a| = |b| = |c| = 1$. Dieser Fall ist durch den Satz 6.20 erledigt.

Nehmen wir jetzt die Richtigkeit des Satzes für alle Gleichungen mit einem Index, der kleiner als K ist, an und weisen seine Richtigkeit für Gleichungen vom Index K nach. Für $K \geqq 2$ kann nicht $|b| = |c|$ sein, da aus $(b, c) = 1$ sofort $|b| = |c| = |a| = 1$ folgt. Also ist $|a| \leqq |b| < |c|$ und $|ab| < |ac| = K \leqq |bc|$.

Da $-ab$ quadratischer Rest modulo c ist, gibt es ganze Zahlen r, q mit

$$ar^2 + b = cq, \qquad |r| \leqq \frac{1}{2}|c|. \tag{16}$$

Für $|q|$ gilt

$$|q| \leqq \frac{|a|\,r^2 + |b|}{|c|} \leqq \frac{1}{4}|ac| + \left|\frac{b}{c}\right| < \frac{K}{4} + 1 < K.$$

Wir unterscheiden zwei Fälle.

1. $q = 0$: Da b quadratfrei und $(a, b) = 1$ ist, folgt aus $b = -ar^2$, daß $b = -a = \pm 1$, $r = \pm 1$ ist. Dann besitzt die Gleichung (15) die Lösungen $x = y = 1$, $z = 0$, und der Satz ist bewiesen.

2. $q \neq 0$: Bezeichnet $A = (ar^2, b, cq)$, so ist nach (16)

$$A = (ar^2, b) = (ar^2, cq) = (b, cq).$$

Aus $A \mid b$ folgt $(A, a) = (A, c) = 1$ und daher $A \mid r^2$ und $A \mid q$. Da b quadratfrei ist, so auch A und $A \mid r$. Wir können daher mit quadratfreiem C

$$r = A\alpha, \qquad b = A\beta, \qquad q = AC\gamma^2 \tag{17}$$

setzen. Aus (16) finden wir

$$aA\alpha^2 + \beta = cC\gamma^2 \tag{18}$$

mit

$$(aA\alpha^2, \beta) = (aA\alpha^2, cC\gamma^2) = (\beta, cC\gamma^2) = 1.$$

Setzen wir noch $B = a\beta$, so ist $ab = AB$.

Wir betrachten jetzt die Gleichung

$$Ax^2 + By^2 + Cz^2 = 0 \tag{19}$$

und zeigen dreierlei: a) Die Gleichung (19) erfüllt sämtliche Bedingungen des Satzes. b) Der Index der Gleichung (19) ist kleiner als K. c) Jede Lösung der Gleichung (19) liefert eine Lösung von (15). Dies vollendet dann den Beweis.

a) Die Gleichung (19) erfüllt sämtliche Bedingungen des Satzes: Es ist $ABC \neq 0$. A und C sind quadratfrei und wegen $AB = ab$ auch B. Überdies ist $(A, B) = 1$. Es gilt $(A, C) = 1$ und wegen $(a, C) = (\beta, C) = 1$ auch $(B, C) = 1$. Ist $ab = AB < 0$, so haben A, B verschiedene Vorzeichen. Es ist dagegen $ab > 0$, so ist $ac < 0$ und $bc < 0$, und wegen (16) ist $q < 0$ und auch $AC < 0$. Also sind die Zahlen A, B, C nicht alle positiv und nicht alle negativ.

Aus (18) folgt

$$a\beta A\alpha^2 + \beta^2 = AB\alpha^2 + \beta^2 \equiv 0 \quad (C),$$

und $-AB$ ist quadratischer Rest modulo C.

Nach (18) ist βcC quadratischer Rest modulo A. Wegen $A \mid b$ ist $-ac$ quadratischer Rest modulo A. Deshalb ist nach

$$(-ac)(\beta cC) = -a\beta c^2 C = -BCc^2$$

$-BC$ quadratischer Rest modulo A.

Nach (18) ist $aAcC$ quadratischer Rest modulo β. Wegen $\beta \mid b$ ist $-ac$ quadratischer Rest modulo β. Deshalb ist $(-ac)(aAcC)$ und auch $-Ac$ quadratischer Rest modulo β. Weiterhin ist nach (18) βcC quadratischer Rest modulo a und folglich auch $(-bc)(\beta cC) = -AC(\beta c)^2$, also auch $-AC$. Wegen $B = a\beta$ und $(a, \beta) = 1$ ist dann $-AC$ quadratischer Rest modulo B.

b) Der Index der Gleichung (19) ist kleiner als K: Da sowohl

$$|AB| = |ab| < |ac| = K$$

als auch

$$|AC| \leqq |AC|\,\gamma^2 = |q| < K$$

ist, fällt jedenfalls der Index der Gleichung (19) kleiner als K aus.

c) Jede Lösung der Gleichung (19) liefert eine Lösung von (15): Nach a) und b) besitzt (19) eine Lösung (x_0, y_0, z_0), die mit $(x_0, y_0, z_0) = 1$ angenommen werden kann. Setzt man

$$x = A\alpha x_0 - \beta y_0, \qquad y = x_0 + a\alpha y_0, \qquad z = C\gamma z_0,$$

so ist

$$\begin{aligned} ax^2 + by^2 + cz^2 &= (aA^2\alpha^2 + b)\, x_0^2 - 2(aA\alpha\beta - ac\alpha)\, x_0 y_0 \\ &\quad + (a\beta^2 + a^2b\alpha^2)\, y_0^2 + cC^2\gamma^2 z_0^2 \\ &= cC\gamma^2(Ax_0^2 + By_0^2 + Cz_0^2) = 0. \end{aligned}$$

Damit ist (x, y, z) eine Lösung von (15) mit $x^2 + y^2 + z^2 > 0$, denn aus $x = y = z = 0$ würde $x_0 = y_0 = z_0 = 0$ folgen.

6.4. Spezielle diophantische Gleichungen dritten und vierten Grades

Das zu Beginn des vorigen Abschnittes bei Kurven zweiter Ordnung demonstrierte Verfahren, aus einem rationalen Punkt durch das Legen von Geraden weitere rationale Punkte zu ermitteln, kann nur sehr bedingt auf Kurven höherer Ordnung übertragen werden, da hier Kurve und Gerade mehr als zwei Schnittpunkte haben können. Betrachten wir Kurven dritter Ordnung. Kennt man auf einer solchen Kurve mit rationalen Koeffizienten zwei rationale Punkte, so kann man durch diese beiden Punkte eine Gerade legen, und der dritte Schnittpunkt mit der Kurve ist notwendig rational. Legt man an einen rationalen Punkt die Tangente, so ist der eventuell noch vorhandene weitere Schnittpunkt mit der Kurve ebenfalls rational. Auf diese Weise kann man sich aus gegebenen rationalen Punkten weitere konstruieren. Aber es ist keineswegs gesagt, daß man dann alle beziehungsweise unendlich viele rationale Punkte erhält.

Das folgende Beispiel (vgl. [13]) soll zeigen, wie aus einem eventuell vorhandenen rationalen Punkt durch fortwährendes Legen von Tangenten unendlich viele rationale Punkte ermittelt werden können. Wir betrachten die Kurve $X^3 + Y^3 = a$ mit $a \in \mathbf{N}$, $a > 2$, und a soll nicht durch die dritte Potenz einer Primzahl teilbar sein. Auf einer solchen Kurve liegen entweder gar keine oder unendlich viele rationale Punkte. Es sei (X_0, Y_0) ein rationaler Punkt der Kurve. Wegen der Voraussetzungen über a ist X_0, $Y_0 \neq 0$ und $X_0 \neq Y_0$. Die Parameterdarstellung der Tangente in diesem Punkt lautet

$$X = X_0 + t, \qquad Y = Y_0 + Y_0' t, \qquad Y_0' = -\left(\frac{X_0}{Y_0}\right)^2.$$

Zur Ermittlung des dritten Schnittpunktes setzen wir in die Kurvengleichung ein und erhalten aus

$$t^3(1 + Y_0'^3) + 3t^2(X_0 + Y_0 Y_0'^2) + 3t(X_0^2 + Y_0^2 Y_0') + X_0^3 + Y_0^3 = a$$

den Parameterwert

$$t = -3\,\frac{X_0 + Y_0 Y_0'^2}{1 + Y_0'^3} = \frac{3X_0 Y_0^3}{X_0^3 - Y_0^3}$$

und die Koordinaten (X_1, Y_1) des Schnittpunktes

$$X_1 = X_0 \frac{X_0^3 + 2Y_0^3}{X_0^3 - Y_0^3}, \qquad Y_1 = -Y_0 \frac{2X_0^3 + Y_0^3}{X_0^3 - Y_0^3}. \tag{20}$$

Daß dieses Verfahren unbegrenzt fortgesetzt zu unendlich vielen rationalen Punkten führt, zeigt der folgende Satz, in dem wir wieder zu homogenen Koordinaten und damit zu ganzzahligen Lösungen übergehen.

Satz 6.22. *Ist $a > 2$ eine natürliche Zahl, die nicht durch die dritte Potenz einer Primzahl teilbar ist, so hat die diophantische Gleichung*

$$x^3 + y^3 = az^3$$

entweder keine oder unendlich viele Lösungen mit $(x, y, z) = 1$ und $z \neq 0$.

Beweis. Es sei (x, y, z) eine Lösung, von der wir sogleich $(x, y) = (y, z) = (z, x) = 1$ annehmen können. Die Beweismethode besteht darin, daß wir aus dieser Lösung eine weitere (x_1, y_1, z_1) mit $|z_1| > |z|$ konstruieren. Das ist aber gleichbedeutend mit der Existenz unendlich vieler Lösungen. Gemäß (20) setzen wir

$$tx_1 = x(x^3 + 2y^3), \qquad ty_1 = -y(2x^3 + y^3), \qquad tz_1 = z(x^3 - y^3)$$

mit

$$t = \big(x(x^3 + 2y^3), y(2x^3 + y^3), z(x^3 - y^3)\big),$$

so daß $(x_1, y_1, z_1) = 1$ ist. Man übersieht schnell die Gleichung $x_1^3 + y_1^3 = az_1^3$. Es kann nicht $x = y$ sein, denn sonst wäre $x = y = \pm 1$, was wegen $a > 2$ nicht geht. Aus $x \neq y$ folgt daher $z_1 \neq 0$. Und da a nicht durch die dritte Potenz einer Primzahl teilbar ist, muß $(x_1, y_1) = (y_1, z_1) = (z_1, x_1) = 1$ sein. Nun überlegen wir uns, welche Werte t annehmen kann. Sei die Primzahl p ein Teiler von t. Aus $p \mid x$ würde $p \mid y$ folgen, was nicht sein kann. Daher ist t ein Teiler von $x^3 + 2y^3$ und $2x^3 + y^3$, also auch von $2(2x^3 + y^3) - (x^3 + 2y^3) = 3x^3$. Damit kann nur $t = 1$ oder $t = 3$ sein. Weiter ist t ein Teiler von $(2x^3 + y^3) - (x^3 + 2y^3) = x^3 - y^3$ und folglich von $x - y$. Das bedeutet $|x - y| \geqq t$ wegen $x \neq y$. Damit haben wir schließlich

$$|z_1| = \left|\frac{z}{t}(x^3 - y^3)\right| \geqq |z(x^2 + xy + y^2)| = \left|\frac{z}{4}\left((2x + y)^2 + 3y^2\right)\right| > |z|.$$

Beispiel. Die Gleichung $x^3 + y^3 = 7z^3$ hat die Lösung $x = 2$, $y = -1$, $z = 1$. Das eben beschriebene Verfahren liefert aus dieser Lösung $t = 3$ und $x_1 = 4$, $y_1 = 5$, $z_1 = 3$.

Von größter Bedeutung für die Entscheidung der Lösbarkeit diophantischer Gleichungen ist eine Umkehrung des geschilderten Verfahrens. Man spricht von der *Fermatschen Methode des unbegrenzten Abstiegs*. Sie kann so beschrieben werden: Wir nehmen an, eine natürliche Zahl n besitze eine gewisse Eigenschaft. Unter dieser Annahme konstruieren wir eine natürliche Zahl $n_1 < n$ mit derselben Eigenschaft. Dies führt aber bei unbegrenzter Weiterführung des Verfahrens zum Widerspruch, da die Menge der natürlichen Zahlen nach unten beschränkt ist. Wir demonstrieren diese Methode an einem Spezialfall des *großen Fermatschen Satzes*.

Es handelt sich um die diophantische Gleichung

$$x^n + y^n = z^n$$

mit natürlicher Zahl $n > 2$. Eine Randnotiz von P. FERMAT in seinem Exemplar der von C. G. BACHET herausgegebenen Werke des DIOPHANTUS besagt, daß diese Gleichung in ganzen von 0 verschiedenen Zahlen keine Lösung besitzt und daß er hierfür einen Beweis habe. Diese Aussage bezeichnet man als *großen Fermatschen Satz*, obwohl der Beweis von P. FERMAT, der aus heutiger Sicht wohl fehlerhaft gewesen sein muß, nie aufgefunden wurde. Der Satz ist auch gegenwärtig nicht vollständig bewiesen, lediglich in einigen Spezialfällen. Wir wollen hier den Spezialfall $n = 4$ sogar in etwas allgemeinerer Gestalt behandeln, der tatsächlich auf P. FERMAT zurückgeht.

Satz 6.23 (FERMAT). *Die diophantische Gleichung*

$$x^4 + y^4 = z^2$$

besitzt keine Lösung in natürlichen Zahlen x, y, z.

Beweis. Wir nehmen eine Lösung in natürlichen Zahlen mit $(x, y, z) = 1$ an. Der gewünschte Widerspruch wird dadurch erzeugt, daß wir aus dieser Lösung eine weitere mit kleinerem z bestimmen werden.

Da x, y nicht beide gerade sein können, nehmen wir ohne Beschränkung der Allgemeinheit $x \equiv 1 \pmod 2$ an. Wegen $x^4 + y^4 \equiv 1, 2 \pmod 4$ und $z^2 \not\equiv 2 \pmod 4$ folgt $z \equiv 1 \pmod 2$ und $y \equiv 0 \pmod 2$. Wir schreiben $(x^2)^2 + (y^2)^2 = z^2$ und wenden Satz 6.20 an. Danach ist

$$x^2 = a^2 - b^2, \qquad y^2 = 2ab, \qquad z = a^2 + b^2$$

mit $a > b > 0$, $(a, b) = 1$, $a \not\equiv b \pmod 2$. Aus $a \equiv 0 \pmod 2$ und $b \equiv 1 \pmod 2$ würde $x^2 \equiv -1 \pmod 4$ folgen, was nicht sein kann. Daher ist $a \equiv 1 \pmod 2$ und $b \equiv 0 \pmod 2$. Wegen

$$\left(\frac{y}{2}\right)^2 = a\,\frac{b}{2}, \qquad \left(a, \frac{b}{2}\right) = 1$$

ist

$$a = z_1^2, \qquad b = 2c^2$$

mit $z_1 > 0$, $c > 0$, $(z_1, c) = 1$, $z_1 \equiv 1 \pmod 2$. Aus

$$x^2 = a^2 - b^2 = z_1^4 - 4c^4$$

folgt

$$x^2 + (2c^2)^2 = (z_1^2)^2$$

mit $(x, 2c, z_1) = 1$. Wir können wiederum Satz 6.20 benutzen und erhalten

$$x = u^2 - v^2, \qquad c^2 = uv, \qquad z_1^2 = u^2 + v^2$$

mit $u > v > 0$, $(u, v) = 1$, $u \not\equiv v \pmod 2$. Aus $c^2 = uv$ und $(u, v) = 1$ ergibt sich $u = x_1^2$, $v = y_1^2$. Damit erfüllen die Werte x_1, y_1, z_1 die Gleichung $x_1^4 + y_1^4 = z_1^2$, und es ist

$(x_1, y_1, z_1) = 1$. Aber

$$z_1 \leqq {z_1}^2 = a \leqq a^2 < a^2 + b^2 = z$$

bringt den Widerspruch.

6.5. Gitterpunkte in ebenen Bereichen

Der Satz 5.37 von C. F. GAUSS besagte, daß die durchschnittliche Größenordnung von $r(n)$ den Wert π hat. Er erlaubt eine geometrische Interpretation. Die Darstellung

$$R(x) = \sum_{k \leqq x} r(k) = \sum_{m^2+n^2 \leqq x} 1$$

läßt sich deuten als die Anzahl der Gitterpunkte (m, n) in und auf einem Kreis mit dem Mittelpunkt im Ursprung und dem Radius $\sqrt{x}$ (Abb. 1). Das Ergebnis des Satzes 5.37

$$R(x) = \pi x + O\left(\sqrt{x}\right)$$

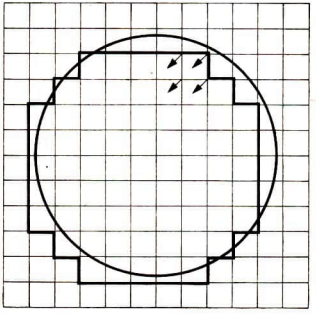

Abb. 1

ist anschaulich sehr plausibel. Ordnet man nämlich jedem Gitterpunkt den Flächeninhalt 1 eines anliegenden Quadrates mit der Seitenlänge 1 zu, so ist die Anzahl der Gitterpunkte im Kreis in erster Näherung gleich dem Flächeninhalt πx. Fehler entstehen bei dieser Betrachtungsweise bei der Einbeziehung der Gitterpunkte in der Nähe des Randes. So ist ein Fehler von der Größenordnung des Umfangs des Kreises in Rechnung zu stellen, was ja auch in der Formel durch $O\left(\sqrt{x}\right)$ zum Ausdruck kommt.

Im nächsten Abschnitt werden wir sehen, daß sich dieses Ergebnis auf weitgehend beliebige Bereiche überträgt. Andererseits kann man damit rechnen, wenn man die Spezifik spezieller Kurven berücksichtigt, daß der Fehler unter Umständen herabgedrückt werden kann. Für dieses Anliegen stellen wir im übernächsten Abschnitt eine elementare Methode von I. M. VINOGRADOV vor, die wir nachfolgend auf spezielle Bereiche anwenden.

6.5.1. Gitterpunkte in allgemeinen Bereichen

In der Ebene sei eine geschlossene Kurve $\mathfrak{C}$ gegeben, die folgenden Eigenschaften genügt (Abb. 2):

(A) $\mathfrak{C}$ ist doppelpunktfrei.

(B) $\mathfrak{C}$ wird von einer vertikalen Geraden höchstens zweimal geschnitten.

(C) Die Funktionen $f_1(t)$ für den oberen Teil der Kurve und $f_2(t)$ für den unteren Teil sind einmal stetig differenzierbar mit eventueller Ausnahme der Randpunkte. Dabei ist $a \leqq t \leqq b_1$

(D) Es existieren die Integrale

$$\int_a^b |f_\nu'(t)|\, dt, \qquad \nu = 1, 2.$$

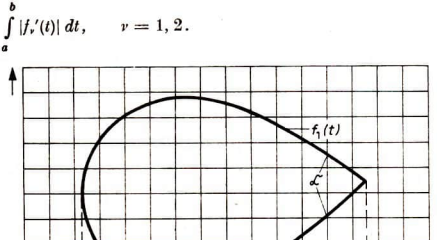

Abb. 2.

Satz 6.24. *Es bezeichne N die Anzahl der Gitterpunkte und F den Flächeninhalt des von der Kurve $\mathfrak{C}$ mit den Eigenschaften* (A) *bis* (D) *und der Länge l ($l > 0$) umschlossenen Bereiches. Dann gilt*

$$N = F + O(l).$$

Beweis. Ohne Beschränkung der Allgemeinheit können wir $0 \leqq a < b$ und $f_\nu(t) > 0$ für $\nu = 1, 2$ annehmen. Rechnen wir die Gitterpunkte auf $\mathfrak{C}$ mit, so bekommen wir

$$N = \sum_{a \leqq n \leqq b} [f_1(n)] - \sum_{a \leqq n \leqq b} [f_2(n)] + O(l).$$

Dabei bezeichnet die erste Summe die Anzahl der Gitterpunkte unterhalb oder auf der Kurve $y = f_1(t)$. Davon subtrahieren wir die Anzahl der Gitterpunkte unterhalb der Kurve $y = f_2(t)$. Da in der zweiten Summe aber die Gitterpunkte auf dieser Kurve mitgezählt werden, müssen wir diesen Wert durch $O(l)$ korrigieren. In beiden Summen wurden die Gitterpunkte auf der t-Achse nicht berücksichtigt. Nun ist

$$N = \sum_{a \leqq n \leqq b} \{f_1(n) - f_2(n)\} + O(l).$$

Die Anwendung der Euler-Maclaurinschen Summenformel gibt mit $f_1(a) = f_2(a)$, $f_1(b) = f_2(b)$, $\psi(t) = t - [t] - 1/2$.

$$N = \int_a^b \{f_1(t) - f_2(t)\}\, dt + \int_a^b \psi(t)\, \{f_1'(t) - f_2'(t)\}\, dt + O(l)$$

$$= F + \int_a^b \psi(t)\, \{f_1'(t) - f_2'(t)\}\, dt + O(l).$$

Für $\nu = 1, 2$ ist

$$\left| \int_a^b \psi(t) f_\nu'(t)\, dt \right| \leqq \frac{1}{2} \int_a^b |f_\nu'(t)|\, dt < \frac{1}{2} \int_a^b \sqrt{1 + f_\nu'^2(t)}\, dt < \frac{l}{2}.$$

Daraus folgt die Behauptung.

Wir betrachten ein Beispiel, welches eine Verallgemeinerung des Kreises darstellt.

Definition 6.3. Es bezeichne $r_{2,k}(n)$ für natürliche Zahlen $k \geqq 2$ die Anzahl der Darstellungen von $n \geqq 0$ in der Form $n = |n_1|^k + |n_2|^k$ mit ganzen Zahlen n_1, n_2. Es sei

$$R_{2,k}(x) = \sum_{n \leqq x} r_{2,k}(n).$$

$R_{2,k}(x)$ gibt die Anzahl der Gitterpunkte in dem von $\mathfrak{C}$ umschlossenen Bereich an, wobei $\mathfrak{C}$ entsprechend den Bezeichnungen des Satzes 6.24 durch

$$f_1(t) = (x - |t|^k)^{1/k}, \qquad f_2(t) = -(x - |t|^k)^{1/k}$$

gegeben ist. Der Flächeninhalt ist

$$F = 4 \int_0^{x^{1/k}} (x - t^k)^{1/k}\, dt = c_k x^{2/k}$$

mit

$$c_k = 4 \int_0^1 (1 - t^k)^{1/k}\, dt. \tag{21}$$

Für denjenigen Leser, der mit der Gammafunktion vertraut ist, sei

$$c_k = \frac{2\Gamma^2\left(\frac{1}{k}\right)}{k\Gamma\left(\frac{2}{k}\right)} \tag{22}$$

hinzugefügt. Die Länge der Kurve ist durch

$$l = 4 \int_0^{x^{1/k}} \sqrt{1 + f_1'^2(t)}\, dt = 4 \int_0^{x^{1/k}} \sqrt{1 + \frac{t^{2k-2}}{(x - t^k)^{2-2/k}}}\, dt = O(x^{1/k})$$

gegeben. Damit ergibt sich

$$R_{2,k}(x) = c_k x^{2/k} + O(x^{1/k}). \tag{23}$$

6.5.2. Die Methode von Vinogradov

Bei der Abschätzung der Anzahl der Gitterpunkte kann man prinzipiell so vorgehen: Man betrachtet die Gitterpunkte auf und unterhalb einer durch $y = f(t) > 0$ gegebenen Kurve bis zur Abszissenachse (ausschließlich) zwischen der Geraden $t = a \geqq 0$ (ausschließlich) und der Geraden $t = b > a$ (einschließlich) (vgl. Abb. 3).

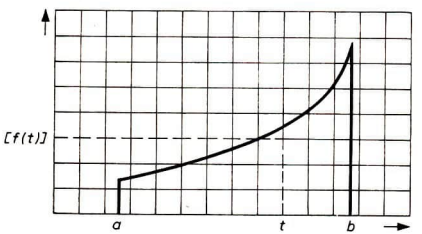

Abb. 3

Ihre Anzahl ist

$$N = \sum_{a<n\leqq b} [f(n)] = \sum_{a<n\leqq b} \left\{f(n) - \frac{1}{2}\right\} - \sum_{a<n\leqq b} \psi(f(n))$$

mit $\psi(x) = x - [x] - \frac{1}{2}$. Die Abschätzung der ersten Summe bietet bei Anwendung der Euler-Maclaurinschen Summenformel keine Schwierigkeiten. Die triviale Abschätzung der zweiten Summe bringt mit $O(b - a)$ die Qualität des vorigen Abschnitts. Da sich aber $\psi(f(n))$ zwischen $-1/2$ und $+1/2$ bewegt, kann man versuchen, die Qualität der Abschätzung durch das Wegheben positiver und negativer Anteile der Summe zu verbessern. Hierauf bezieht sich die Vinogradovsche Methode. Wir folgen der Darstellung in [6] und beginnen mit zwei Hilfssätzen.

Hilfssatz 6.8. *Es seien n natürliche Zahlen $x_1, x_2, \ldots, x_n$ mit $x_i \leqq N$ $(i = 1, 2, \ldots, n)$ gegeben. Dann kann man diese Folge ohne Änderung der Anordnung mit Ausnahme von weniger als N Elementen in Klassen mit folgender Eigenschaft zerlegen: Die Anzahl m der Elemente einer solchen Klasse $x_{a+1}, x_{a+2}, \ldots, x_{a+m}$ ist gleich der größten in ihr enthaltenen Zahl.*

Beweis. Da der Hilfssatz für $n < N$ trivial ist, können wir gleich $n \geqq N$ annehmen. Wir betrachten die ersten x_1 Elemente $x_1, x_2, \ldots, x_{x_1}$ der gegebenen Folge

und bezeichnen mit $x^{(2)}$ die größte enthaltene Zahl. Es kann nur $x^{(2)} = x_1$ oder $x^{(2)} > x_1$ sein. Ist $x^{(2)} = x_1$, dann bilden diese Elemente eine Klasse im Sinne des Hilfssatzes. Ist $x^{(2)} > x_1$, dann betrachten wir die Elemente $x_1, x_2, \ldots, x_{x^{(2)}}$ und bezeichnen mit $x^{(3)}$ die größte Zahl von diesen Elementen. Für $x^{(3)} = x^{(2)}$ erhalten wir eine gewünschte Klasse. Für $x^{(3)} > x^{(2)}$ setzen wir das Verfahren fort und betrachten $x_1, x_2, \ldots, x_{x^{(3)}}$. Man erhält so eine Folge von Elementefolgen, deren Elementeanzahl eine streng monoton wachsende Folge bildet: $x_1 < x^{(2)} < x^{(3)} < \cdots$. Da alle $x_i \leqq N$ sind, kann diese Folge nicht mehr als N Glieder haben. Man gelangt also nach höchstens N Schritten zu einer Klasse, die den Erfordernissen des Hilfssatzes genügt.

Bleiben hernach weniger als N Elemente übrig, so ist der Hilfssatz bewiesen. Im anderen Fall bilden wir eine zweite Klasse, indem wir nach dem letzten erfaßten Element in gleicher Weise fortfahren und so weiter.

Hilfssatz 6.9. *Es seien x, y, a ganze Zahlen mit $x > 0$, $(x, y) = 1$. Für die Funktion $g(n)$ gelte $|g(\alpha) - g(\beta)| < C$ für $\alpha, \beta \in \{a+1, a+2, \ldots, a+x\}$. Dann ist mit*

$$\psi(x) = x - [x] - \frac{1}{2}$$

$$\left| \sum_{m=a+1}^{a+x} \psi\left(\frac{ym + g(m)}{x}\right) \right| \leqq C + \frac{1}{2}.$$

Beweis. Es sei

$$S = \sum_{m=a+1}^{a+x} \psi\left(\frac{ym + g(m)}{x}\right).$$

Wir unterscheiden zwei Fälle:

1. $C + \frac{1}{2} \geqq \frac{x}{2}$: Hier gibt die triviale Abschätzung $|S| \leqq \frac{x}{2} \leqq C + \frac{1}{2}$ sofort die Behauptung.

2. $C + \frac{1}{2} < \frac{x}{2}$: Es bezeichne q den kleinsten Wert von $g(m)$ für $m \in \{a+1, a+2, \ldots, a+x\}$ und $g(m) = q + g_1(m)$, so daß für diese Werte von m die Ungleichung $0 \leqq g_1(m) \leqq C$ besteht. In S ersetzen wir $ym + [q]$ durch seinen kleinsten, nicht negativen Rest u modulo x. Damit wird

$$S = \sum_{u=0}^{x-1} \psi\left(\frac{u + q - [q] + g_2(u)}{x}\right)$$

mit $0 \leqq g_2(u) \leqq C$. Wir zerlegen die Summe in zwei Teilsummen. In die erste Teilsumme nehmen wir alle Glieder mit $0 \leqq u < x - C - q + [q]$ und in die zweite Teilsumme alle Glieder mit $x - C - q + [q] \leqq u < x$ auf. Für die Glieder der ersten Teilsumme ist

$$0 \leqq \frac{u + q - [q] + g_2(u)}{x} < 1,$$

und für die Glieder der zweiten Teilsumme ergibt sich bei Berücksichtigung von $C + \frac{1}{2} < \frac{x}{2}$

$$0 < \frac{u + q - [q] + g_2(u)}{x} < 2.$$

Setzen wir

$$\psi\left(\frac{u + q - [q] + g_2(u)}{x}\right) = \frac{u + q - [q] + g_2(u)}{x} - \frac{1}{2} + h(u),$$

so ist $h(u) = 0$ für die erste Teilsumme und $h(u) = 0$ oder $h(u) = -1$ für die zweite Teilsumme. Da die zweite Teilsumme höchstens $C + q - [q]$ Glieder enthält, folgt

$$\sum_{u=0}^{x-1} \left(\frac{u + q - [q] + g_2(u)}{x} - \frac{1}{2}\right) - C - q + [q] \leqq S$$
$$\leqq \sum_{u=0}^{x-1} \left(\frac{u + q - [q] + g_2(u)}{x} - \frac{1}{2}\right).$$

Mit $0 \leqq g_2(u) \leqq C$ ergibt sich hieraus

$$-\frac{1}{2} - C \leqq S \leqq \frac{1}{2} + C.$$

Satz 6.25 (Vinogradov). *Es seien a, b, h, z reelle Zahlen mit $a < b, h \geqq 1, z > 29$. Für $a \leqq t \leqq b$ sei $f(t)$ zweimal stetig differenzierbar, und es sei $\frac{1}{hz} \leqq f''(t) \leqq \frac{1}{z}$ bzw. $\frac{1}{hz} \leqq -f''(t) \leqq \frac{1}{z}$. Dann ist*

$$\left| \sum_{a < n \leqq b} \psi(f(n)) \right| < 2h\left(\frac{b - a}{z} + 1\right)(z \log z)^{2/3}. \tag{24}$$

Beweis. Wir führen den Beweis in mehreren Schritten. Dabei können wir ohne weiteres $b - a > 2$ annehmen.

1. Ist $a < n \leqq b - 1$, so folgt aus $f'(n + 1) - f'(n) = f''(n + \vartheta)$ $(0 < \vartheta < 1)$ entweder stets

$$\frac{1}{hz} \leqq f'(n + 1) - f'(n) \leqq \frac{1}{z}$$

oder

$$\frac{1}{hz} \leqq f'(n) - f'(n + 1) \leqq \frac{1}{z}.$$

Ist k die kleinste der Zahlen $f'(n)$ mit $a < n \leqq b$, dann ist die größte kleiner als $k + \frac{b - a}{z}$. Die Anzahl der Zahlen $f'(n)$ mit $c \leqq f'(n) \leqq d$ ist höchstens $hz(d - c) + 1$.

2. Wir führen eine Zahl τ ein, die zunächst nur der Ungleichung $4 < \tau < \sqrt{z}$ genügen soll. Später werden wir sie präzisieren. Nach Satz 4.7 gibt es ein Paar ganzer Zahlen $x(n), y(n)$ mit

$$|x(n)\, f'(n) - y(n)| < \frac{1}{\tau},$$

$\big(x(n), y(n)\big) = 1$ und $0 < x(n) \leqq \tau$. Nunmehr teilen wir die Zahlen $x([a]+1)$, $x([a]+2), \ldots, x([b])$ gemäß Hilfssatz 6.8 mit Ausnahme von höchstens τ Zahlen in Klassen ein. Eine solche Klasse sei durch $x(\alpha_\nu + 1), x(\alpha_\nu + 2), \ldots, x(\alpha_\nu + n_\nu)$ gegeben. In ihr befindet sich eine Zahl $x(\beta_\nu)$ mit $x(\beta_\nu) = n_\nu$. Hierfür gilt

$$|n_\nu f'(\beta_\nu) - y(\beta_\nu)| < \frac{1}{\tau}, \qquad 0 < n_\nu \leqq \tau,$$

$$f'(\beta_\nu) = \frac{y(\beta_\nu)}{n_\nu} + \frac{\theta}{\tau n_\nu}, \qquad |\theta| < 1. \tag{25}$$

3. Wir betrachten die Summe

$$S_\nu = \sum_{n=\alpha_\nu+1}^{\alpha_\nu+n_\nu} \psi\big(f(n)\big),$$

setzen $n = \beta_\nu + m$ und benutzen die Taylorentwicklung von $f(n)$. Wir erhalten

$$S = \sum_{m=\alpha_\nu-\beta_\nu+1}^{\alpha_\nu-\beta_\nu+n_\nu} \psi\left(f(\beta_\nu) + mf'(\beta_\nu) + \frac{m^2}{2} f''(\beta_\nu + m\varrho)\right)$$

mit $\varrho = \varrho(m)$ und $|\varrho(m)| < 1$. Wegen $\alpha_\nu + 1 \leqq \beta_\nu \leqq \alpha_\nu + n_\nu$ ist $-n_\nu < m < n_\nu$. Nach Voraussetzung ist

$$\frac{m^2}{2hz} \leqq \pm\frac{m^2}{2} f''(\beta_\nu + m\varrho) \leqq \frac{m^2}{2z}.$$

Setzen wir

$$\pm\frac{m^2}{2} f''(\beta_\nu + m\varrho) = \frac{n_\nu^2}{2z}\sigma(m),$$

so ist $0 \leqq \sigma(m) < 1$. Verwenden wir dies und (25), so entsteht

$$S_\nu = \sum_{m=\alpha_\nu-\beta_\nu+1}^{\alpha_\nu-\beta_\nu+n_\nu} \psi\left(\frac{n_\nu f(\beta_\nu) + my(\beta_\nu) + \dfrac{\theta m}{\tau} \pm \dfrac{n_\nu^3}{2z}\sigma(m)}{n_\nu}\right).$$

Hierauf kann Hilfssatz 6.9 angewandt werden. Mit den dortigen Bezeichnungen ist $x = n_\nu$, $y = y(\beta_\nu)$, $a = \alpha_\nu - \beta_\nu$,

$$g(m) = n_\nu f(\beta_\nu) + \frac{\theta m}{\tau} \pm \frac{n_\nu^3}{2z}\sigma(m),$$

so daß sich

$$C = \frac{n_\nu}{\tau} + \frac{n_\nu^3}{2z}$$

als geeignet erweist. Folglich ist

$$|S_\nu| < \frac{n_\nu}{\tau} + \frac{n_\nu^3}{2z} + \frac{1}{2}.$$

4. Nun schreiben wir

$$\sum_{a<n\leqq b} \psi\big(f(n)\big) = \sum_\nu S_\nu + \sum_r \psi\big(f(r)\big).$$

Dabei ist die Summe über ν entsprechend der in Teil 2 vorgenommenen Klasseneinteilung zu bilden. Die Summe über r wird über diejenigen Zahlen erstreckt, die sich der Klasseneinteilung entziehen, von denen es aber höchstens τ Zahlen gibt. Daher ist

$$\left|\sum_{a<n\leqq b} \psi\big(f(n)\big)\right| < \sum_\nu \left(\frac{n_\nu}{\tau} + \frac{n_\nu^3}{2z} + \frac{1}{2}\right) + \frac{\tau}{2}$$

und wegen $n_\nu \leqq \tau$, $4 < \tau < \sqrt{z}$

$$\begin{aligned}\left|\sum_{a<n\leqq b} \psi\big(f(n)\big)\right| &< \left(\frac{1}{\tau} + \frac{\tau^2}{2z}\right)(b-a+1) + \frac{\tau}{2} + \frac{T}{2} \\ &< \left(\frac{1}{\tau} + \frac{\tau^2}{2z}\right)(b-a) + \tau + \frac{T}{2}. \qquad (26)\end{aligned}$$

Hierin bedeutet T die Anzahl der Klassen.

5. Für die Zahlen $x(\alpha_\nu + 1), x(\alpha_\nu + 2), \ldots, x(\alpha_\nu + n_\nu)$ gilt

$$\sum_{n=\alpha_\nu+1}^{\alpha_\nu+n_\nu} \frac{1}{x(n)} \geqq \sum_{n=\alpha_\nu+1}^{\alpha_\nu+n_\nu} \frac{1}{n_\nu} = 1.$$

Deshalb haben wir für die Anzahl T aller Klassen

$$T \leqq \sum_{a<n\leqq b} \frac{1}{x(n)}.$$

Jetzt ist festzustellen, wie oft sich derselbe Wert $x(n)$ in der Summe wiederholt. Zu gegebenem x können nur solche Werte y gehören, für die

$$|xf'(n) - y| < \frac{1}{\tau}$$

gilt. Bezeichnet k die kleinste der Zahlen $f'(n)$, so folgt daraus und nach Teil 1

$$\begin{aligned}&xf'(n) - \frac{1}{\tau} < y < xf'(n) + \frac{1}{\tau}, \\ &kx - \frac{1}{\tau} < y < \left(k + \frac{b-a}{z}\right)x + \frac{1}{\tau}.\end{aligned}$$

Die Anzahl der möglichen Zahlen y ist deshalb höchstens

$$\frac{b-a}{z}x+\frac{2}{\tau}+1<\frac{b-a}{z}x+\frac{3}{2}.$$

Zu einem gegebenen Paar x, y können nur solche Werte $f'(n)$ gehören, für die

$$\frac{1}{x}\left(y-\frac{1}{\tau}\right)<f'(n)<\frac{1}{x}\left(y+\frac{1}{\tau}\right)$$

gilt. Nach Teil 1 ist die Anzahl dieser Zahlen $f'(n)$ höchstens

$$\frac{2hz}{\tau x}+1<\frac{3hz}{\tau x}$$

wegen $x<\tau<\sqrt{z}$, $h\geqq 1$. Insgesamt können zu einem gegebenen x höchstens

$$\left(\frac{b-a}{z}x+\frac{3}{2}\right)\frac{3hz}{\tau x}$$

Zahlen $f'(n)$ gehören. Daher ist

$$T<h\sum_{0<x<\tau}\left(3\,\frac{b-a}{\tau}+\frac{9z}{2\tau x}\right)\frac{1}{x}.$$

Mit

$$\sum_{0<x<\tau}\frac{1}{x}<\log\tau+1<\frac{1}{2}\log z+1,$$

$$\sum_{0<x<\tau}\frac{1}{x^2}<\sum_{x=1}^{\infty}\frac{1}{x^2}=\frac{\pi^2}{6}<\frac{5}{3}$$

ergibt sich

$$T<h\left(\frac{3}{2}\,\frac{b-a}{\tau}\log z+3\,\frac{b-a}{\tau}+\frac{15}{2}\,\frac{z}{\tau}\right).$$

6. Setzt man diese Abschätzung in (26) ein, so erhält man

$$\left|\sum_{a<n\leqq b}\psi(f(n))\right|<h(b-a)\left(\frac{5}{2\tau}+\frac{\tau^2}{2z}+\frac{3}{4\tau}\log z\right)+\frac{15hz}{4\tau}+\tau.$$

Diese Abschätzung wird besonders günstig, wenn man noch $\tau=(z\log z)^{1/3}$ wählt, wobei mit $z>29$ die Bedingung $4<\tau<\sqrt{z}$ sicher erfüllt ist. Somit wird für $z>29$

$$\left|\sum_{a<n\leqq b}\psi(f(n))\right|<2h\left(\frac{b-a}{z}+1\right)(z\log z)^{2/3}.$$

Es sollen jetzt einige Anwendungen des Vinogradovschen Satzes gegeben werden, die wir in der Form von Hilfssätzen formulieren, da sie in den nächsten beiden Abschnitten benötigt werden.

Hilfssatz 6.10. *Für $x \to \infty$ ist*

$$\sum_{0 \leqq n \leqq \sqrt{\frac{x}{2}}} \psi\left(\sqrt{x - n^2}\right) = O\left(x^{1/3} (\log x)^{2/3}\right).$$

Beweis. Mit den Bezeichnungen des Satzes 6.25 ist

$$f(t) = (x - t^2)^{1/2}, \qquad f''(t) = -x(x - t^2)^{-3/2}$$

und im Intervall $0 \leqq t \leqq \sqrt{\frac{x}{2}}$

$$\frac{1}{\sqrt{x}} \leqq -f''(t) \leqq 2^{3/2} \frac{1}{\sqrt{x}}.$$

Daher ist $z = 2^{-3/2}\sqrt{x} > 29$, $h = 2^{3/2}$,

$$\frac{b-a}{z} = 2^{3/2} \frac{1}{\sqrt{x}} \sqrt{\frac{x}{2}} = O(1).$$

Aus (24) ergibt sich sofort die Behauptung.

Hilfssatz 6.11. *Es sei k eine natürliche Zahl mit $k \geqq 2$. Für $x \to \infty$ ist*

$$\sum_{\frac{x}{2} < n^k \leqq x} \psi\left((x - n^k)^{1/k}\right) = O\left(x^{2/3k} (\log x)^{2/3}\right).$$

Beweis. Es ist

$$f(t) = (x - t^k)^{1/k}, \qquad f''(t) = -(k-1)\, x t^{k-2} (x - t^k)^{\frac{1}{k} - 2}.$$

Da $f''(t)$ für $t^k \to x$ gegen $-\infty$ strebt, können wir nicht so rasch wie im vorigen Beispiel den Vinogradovschen Satz anwenden. Wir werden uns an die Stelle $t^k = x$ herantasten und bilden mit noch geeignet zu wählendem y

$$\sum_{x/2 < n^k \leqq x} \psi\left(f(n)\right) = S_1 + S_2,$$

$$S_1 = \sum_{1 \leqq \nu < y} T_\nu, \qquad S_2 = \sum_{\nu \geqq y} T_\nu,$$

$$T_\nu = \sum_{x(1-2^{-\nu}) < n^k \leqq x(1-2^{-\nu-1})} \psi\left(f(n)\right).$$

Die in S_1 auftretenden Summen T_ν werden mit der Vinogradovschen Methode, S_2 später trivial abgeschätzt. Für die Anwendung des Satzes 6.25 auf T_ν in S_1 ist

$$a = \left(x(1 - 2^{-\nu})\right)^{1/k}, \qquad b = \left(x(1 - 2^{-\nu-1})\right)^{1/k},$$

$$-f''(t) \leqq (k-1)\, x^{-\frac{1}{k}} (1 - 2^{-\nu-1})^{1 - \frac{2}{k}}\, 2^{(\nu+1)\left(2 - \frac{1}{k}\right)} \leqq (k-1)\, 2^{(\nu+1)\left(2-\frac{1}{k}\right)}\, x^{-\frac{1}{k}}$$

$$-f''(t) \geqq (k-1)\, x^{-\frac{1}{k}} (1 - 2^{-\nu})^{1 - \frac{2}{k}}\, 2^{\nu\left(2 - \frac{1}{k}\right)} \geqq (k-1)\, 2^{\frac{2}{k} - 1}\, 2^{\nu\left(2 - \frac{1}{k}\right)}\, x^{-\frac{1}{k}}.$$

Für h und z finden wir hieraus

$$h = 2^{3-\frac{3}{k}}, \qquad z = \frac{1}{k-1}\, 2^{(\nu+1)\left(\frac{1}{k}-2\right)}\, x^{1/k}.$$

Wählt man x hinreichend groß, so ist für alle $\nu < y$ die Ungleichung $z \geqq 29$ gesichert, falls wir

$$2^y = cx^{\frac{1}{2k-1}}$$

mit einer geeigneten Konstanten c festlegen. Weiter ist

$$\frac{b-a}{z} = (k-1)\, 2^{(\nu+1)\left(2-\frac{1}{k}\right)} \left((1-2^{-\nu-1})^{1/k} - (1-2^{-\nu})^{1/k}\right) = O\left(2^{\nu\left(1-\frac{1}{k}\right)}\right).$$

Damit ergibt sich aus (24)

$$T_\nu = O\left(2^{-\frac{\nu}{3}\left(1+\frac{1}{k}\right)} x^{\frac{2}{3k}} (\log x)^{2/3}\right),$$

und da für die Abschätzung von S_1 über ν bis ∞ summiert werden kann

$$S_1 = O\left(x^{\frac{2}{3k}} (\log x)^{2/3}\right).$$

Durch triviale Abschätzung von S_2 erhalten wir

$$\begin{aligned} |S_2| = \left| \sum_{x(1-2^{-\nu}) < n^k \leqq x} \psi(f(n)) \right| &\leqq \frac{1}{2}\left[x^{1/k}\right] - \frac{1}{2}\left[x(1-2^{-\nu})^{1/k}\right] \\ &\leqq \frac{1}{2}\, x^{1/k} - \frac{1}{2}\left(x(1-2^{-\nu})\right)^{1/k} + \frac{1}{2} \\ &= O(x^{1/k} 2^{-\nu}) = O\left(x^{\frac{1}{k}-\frac{1}{2k-1}}\right). \end{aligned}$$

Wegen

$$\frac{1}{k} - \frac{1}{2k-1} < \frac{2}{3k}$$

ergibt sich aus den Abschätzungen von S_1 und S_2 die Behauptung.

Hilfssatz 6.12. *Ist* $y \geqq 1$, $r > 0$, $1 \leqq A < B$, $A^{r+2} > 29r(r+1)\, y$, *dann gilt*

$$\sum_{A < k \leqq B} \psi\left(\frac{y}{k^r}\right) = O\left(y^{-2/3} B^{\frac{2(r+2)}{3}} (\log B)^{2/3}\right) + \begin{cases} O\left(y^{1/3} B^{\frac{1-r}{3}} (\log B)^{2/3}\right) & \text{für } r < 1, \\ O\left(y^{1/3} (\log B)^{5/3}\right) & \text{für } r = 1, \\ O\left(y^{1/3}\, A^{\frac{1-r}{3}} (\log B)^{2/3}\right) & \text{für } r > 1. \end{cases}$$

Beweis. Die natürliche Zahl N sei so gewählt, daß $A2^{N-1} < B \leqq A2^N$ gilt. Dann ist

$$\sum_{A<k\leqq B} \psi\left(\frac{y}{k^r}\right) = \sum_{\nu=0}^{N-2} R_\nu + R$$

mit

$$R_\nu = \sum_{A2^\nu<k\leqq A2^{\nu+1}} \psi\left(\frac{y}{k^r}\right), \qquad R = \sum_{A2^{N-1}<k\leqq B} \psi\left(\frac{y}{k^r}\right).$$

Für $N = 1$ entfällt dabei die Summe auf der rechten Seite. Wir wenden auf R_ν und R Satz 6.25 an. Für die Summe R_ν ist

$$a = A2^\nu, \qquad b = A2^{\nu+1}, \qquad f(t) = yt^{-r}, \qquad f''(t) = r(r+1)\,yt^{-r-2},$$
$$\frac{r(r+1)\,y}{2^{r+2}\,(A2^\nu)^{r+2}} \leqq f''(t) \leqq \frac{r(r+1)\,y}{(A2^\nu)^{r+2}},$$
$$z = \frac{(A2^\nu)^{r+2}}{r(r+1)\,y}, \qquad h = 2^{r+2}, \qquad \frac{b-a}{z} = \frac{r(r+1)\,y}{(A2^\nu)^{r+1}}.$$

Dies gilt alles auch für die Summe R, wenn man $\nu = N-1$ und $b = B \leqq A2^N$ setzt. Für $\dfrac{b-a}{z}$ erhält man den angegebenen Wert als obere Schranke. Somit ist

$$\sum_{A<k\leqq B} \psi\left(\frac{y}{k^r}\right) = \sum_{\nu=0}^{N+1} \left\{O\left(y^{1/3}\,(A2^\nu)^{\frac{1-r}{3}}\right) + O\left(y^{-2/3}\,(A2^\nu)^{\frac{2(r+2)}{3}}\right)\right\} (\log B)^{2/3}.$$

Die Auswertung der Summe über ν gibt die Behauptung.

6.5.3. Das Kreisproblem und Verallgemeinerungen

Mit Hilfe der Vinogradovschen Methode geben wir eine Verbesserung der Abschätzung des Satzes 5.37.

Satz 6.26. *Für die Anzahl der Gitterpunkte $R(x)$ im Kreis $\xi^2 + \eta^2 \leqq x$ gilt*

$$R(x) = \pi x + O\left(x^{1/3}(\log x)^{2/3}\right).$$

Beweis. Es ist

$$R(x) = \sum_{n^2+m^2\leqq x} 1 = 1 + 4\left[\sqrt{x}\right] + 4 \sum_{\substack{n^2+m^2\leqq x \\ n,m\geqq 1}} 1$$
$$= 1 + 4\left[\sqrt{x}\right] + 4 \sum_{\substack{n^2+m^2\leqq x \\ 1\leqq m^2\leqq \frac{x}{2}, n\geqq 1}} 1 + 4 \sum_{\substack{n^2+m^2\leqq x \\ m^2>\frac{x}{2}, n\geqq 1}} 1$$
$$= 1 + 4\left[\sqrt{x}\right] + 4 \sum_{1\leqq m^2\leqq \frac{x}{2}} \left[\sqrt{x-m^2}\right] + 4 \sum_{1\leqq n^2\leqq \frac{x}{2}} \left\{\left[\sqrt{x-n^2}\right] - \left[\sqrt{\frac{x}{2}}\right]\right\}$$
$$= 1 + 4\left[\sqrt{x}\right] - 4\left[\sqrt{\frac{x}{2}}\right]^2 + 8 \sum_{1\leqq n^2\leqq \frac{x}{2}} \left[\sqrt{x-n^2}\right].$$

Mit $\psi(y) = y - [y] - \frac{1}{2}$ ergibt sich

$$R(x) = -2x + 4\sqrt{x} + 8\sqrt{\frac{x}{2}}\,\psi\left(\sqrt{\frac{x}{2}}\right) + 8\sum_{1\leqq n^2\leqq \frac{x}{2}}\sqrt{x-n^2} - 8\sum_{1\leqq n^2\leqq\frac{x}{2}}\psi\left(\sqrt{x-n^2}\right) + O(1).$$

Die Anwendung der Euler-Maclaurinschen Summenformel liefert

$$R(x) = -2x + 8\int_0^{\sqrt{x/2}}\sqrt{x-t^2}\,dt - 8\int_0^{\sqrt{x/2}}\frac{t\psi(t)}{\sqrt{x-t^2}}\,dt - 8\sum_{n^2\leqq\frac{x}{2}}\psi\left(\sqrt{x-n^2}\right) + O(1).$$

Das zweite Integral schätzen wir durch partielle Integration zu $O(1)$ ab. Somit folgt

$$\begin{aligned} R(x) &= 4\int_0^{\sqrt{x}}\sqrt{x-t^2}\,dt - 8\sum_{n^2\leqq\frac{x}{2}}\psi\left(\sqrt{x-n^2}\right) + O(1) \\ &= \pi x - 8\sum_{n^2\leqq\frac{x}{2}}\psi\left(\sqrt{x-n^2}\right) + O(1). \end{aligned}$$

Hilfssatz 6.10 gibt nun die Behauptung.

Als *Kreisproblem* bezeichnet man die Aufgabe, das Infimum, $\vartheta = \inf\alpha$, in der Abschätzung

$$R(x) = \pi x + O(x^{\alpha})$$

zu bestimmen. Historisch gesehen nahm dieses Problem seinen Ausgangspunkt bei C. F. Gauss, der $\vartheta \leqq \frac{1}{2}$, das ist unser Satz 5.37, bewies. Ganz einfach kann man auch $\vartheta \geqq 0$ zeigen, wie folgender Satz belegt.

Satz 6.27. *Die Gleichung*

$$R(x) = \pi x + o(1)$$

ist falsch.

Beweis. Wir nehmen an, es sei $R(x) = \pi x + o(1)$ richtig. Dann ist mit einer natürlichen Zahl n

$$0 = R\left(n+\frac{1}{2}\right) - R(n) = \pi\left(n+\frac{1}{2}\right) - \pi n + o(1) = \frac{\pi}{2} + o(1),$$

was einen offensichtlichen Widerspruch darstellt.

Den ersten Fortschritt gegenüber dem klassischen Resultat erzielte W. Sierpiński, der 1906 nach einer Methode von G. F. Voronoi $\vartheta \leqq \frac{1}{3}$ zeigte. Sein Beweis wurde im Laufe der Jahre stark vereinfacht, und I. M. Vinogradov konnte 1917 diese Abschätzung bis auf einen logarithmischen Faktor sogar elementar beweisen, wie wir gesehen haben. G. H. Hardy und

E. Landau wiesen 1915 $\vartheta \geqq \frac{1}{4}$ nach, was man nach einer 1956 von P. Erdös und W. H. J. Fuchs entwickelten Methode jetzt auch elementar beweisen kann. Diese untere Abschätzung steht heute noch. Hinsichtlich der oberen Abschätzung setzte mit den grundlegenden Arbeiten J. G. van der Corput (1890–1975) in den zwanziger Jahren eine stürmische Entwicklung ein. Er unterbot 1923 als erster die ominöse Zahl $\frac{1}{3}$ und erreichte $\vartheta \leqq \frac{37}{112}$. Zahlreiche Autoren verbesserten in den folgenden Jahren diese Abschätzung. Das beste Resultat steht bei $\vartheta \leqq \frac{12}{37}$ und stammt von Wen-Lin Yin aus dem Jahre 1962.

Als Verallgemeinerung des Kreisproblems betrachten wir jetzt die in Definition 6.3 gegebene Funktion $R_{2,k}(x)$. Gegenüber der Abschätzung (23) zeigte 1966 B. Randol

$$R_{2,k}(x) = c_k x^{2/k} + O\left(x^{\frac{1}{k}-\frac{1}{k^2}}\right)$$

für gerade $k > 2$ und auch, daß diese Abschätzung nicht mehr zu verbessern ist. Wir zeigen noch weit mehr:

Erstens gilt diese Aussage auch für ungerade k. Zweitens kann man dieses Ergebnis dahingehend verbessern, daß man noch eine Funktion der genannten Größenordnung präzis angeben kann und dann den Rest noch weiter abschätzt. Es handelt sich um die Funktion

$$\varrho_k(x) = -8 \int_0^x t^{k-1}(x^k - t^k)^{\frac{1}{k}-1} \psi(t)\, dt, \tag{27}$$

$k \in \mathbf{N}$, $k \geqq 2$, $\psi(t) = t - [t] - \frac{1}{2}$ mit $x^{1/k}$ anstelle von x. Wir zeigen zunächst, daß $\varrho_k(x)$ von der behaupteten Größenordnung ist.

Hilfssatz 6.13. *Für $x \to \infty$ ist*

$$\varrho_k(x) = O\left(x^{1-\frac{1}{k}}\right).$$

Beweis. Wir bilden mit $y^k = x^k - x^{k-1}$

$$\varrho_k(x) = I_1 + I_2,$$

$$I_1 = -8 \int_0^y t^{k-1}(x^k - t^k)^{\frac{1}{k}-1} \psi(t)\, dt,$$

$$I_2 = -8 \int_y^x t^{k-1}(x^k - t^k)^{\frac{1}{k}-1} \psi(t)\, dt$$

und schätzen die Integrale einzeln ab. Mit $\psi_1(t) = \int_0^t \psi(\tau)\, d\tau$ ist

$$I_1 = -8y^{k-1}(x^k - y^k)^{\frac{1}{k}-1} \psi_1(y) + 8 \int_0^y \frac{d}{dt}\left\{t^{k-1}(x^k - t^k)^{\frac{1}{k}-1}\right\} \psi_1(t)\, dt$$

$$= O\left(y^{k-1}(x^k - y^k)^{\frac{1}{k}-1}\right) = O\left(x^{1-\frac{1}{k}}\right).$$

Für I_2 erhalten wir aus

$$|I_2| \leqq 4 \int_y^x t^{k-1}(x^k - t^k)^{\frac{1}{k}-1}\, dt = 4(x^k - y^k)^{1/k}$$

$$I_2 = O\left(x^{1-\frac{1}{k}}\right).$$

Daraus folgt die Behauptung.

Satz 6.28 (Krätzel). *Für $k = 3$ ist*

$$R_{2,3}(x) = c_3 x^{2/3} + O\left(x^{2/9}(\log x)^{2/3}\right)$$

und für $k > 3$

$$R_{2,k}(x) = c_k x^{2/k} + \varrho_k(x^{1/k}) + O\left(x^{2/3k}(\log x)^{2/3}\right)$$

mit der durch (27) gegebenen Funktion $\varrho_k(x)$ und

$$c_k = \frac{2\Gamma^2\left(\frac{1}{k}\right)}{k\Gamma\left(\frac{2}{k}\right)}.$$

Bemerkung. Bei Heranziehung schärferer Methoden kann man die Abschätzung noch so weit verbessern, daß man auch im Fall $k = 3$ die Funktion $\varrho_3(x^{1/3}) = O(x^{2/9})$ explizit herausziehen kann.

Beweis. Wir gehen prinzipiell wie im Beweis zu Satz 6.26 vor, modifizieren aber etwas im Hinblick auf die Anwendung des Hilfssatzes 6.11

$$\begin{aligned} R_{2,k}(x) &= \sum_{|n|^k+|m|^k \leqq x} 1 = 1 + 4[x^{1/k}] + 4 \sum_{\substack{n^k+m^k \leqq x \\ n,m \geqq 1}} 1 \\ &= 1 + 4[x^{1/k}] + 4 \sum_{\substack{n^k+m^k \leqq x \\ m^k > \frac{x}{2}}} 1 + 4 \sum_{\substack{n^k+m^k \leqq x \\ 1 \leqq m^k \leqq \frac{x}{2}}} 1 \\ &= 1 + 4[x^{1/k}] + 4\left[\left(\frac{x}{2}\right)^{1/k}\right]^2 + 8 \sum_{\substack{n^k+m^k \leqq x \\ m^k > \frac{x}{2}}} 1 \\ &= 1 + 4[x^{1/k}] + 4\left[\left(\frac{x}{2}\right)^{1/k}\right]^2 + 8 \sum_{\frac{x}{2} < m^k \leqq x} [(x - m^k)^{1/k}]. \end{aligned}$$

Mit $\psi(y) = y - [y] - \frac{1}{2}$ ergibt sich

$$\begin{aligned} R_{2,k}(x) = 4\left(\frac{x}{2}\right)^{2/k} &- 8\left(\frac{x}{2}\right)^{1/k} \psi\left(\left(\frac{x}{2}\right)^{1/k}\right) + 8 \sum_{\frac{x}{2} < m^k \leqq x} (x - m^k)^{1/k} \\ &- 8 \sum_{\frac{x}{2} < m^k \leqq x} \psi\left((x - m^k)^{1/k}\right) + O(1). \end{aligned}$$

Die Anwendung der Euler-Maclaurinschen Summenformel liefert

$$R_{2,k}(x) = 4\left(\frac{x}{2}\right)^{2/k} + 8\int_{\left(\frac{x}{2}\right)^{1/k}}^{x^{1/k}} (x - t^k)^{1/k}\,dt - 8\int_{\left(\frac{x}{2}\right)^{1/k}}^{x^{1/k}} t^{k-1}(x - t^k)^{\frac{1}{k}-1}\,\psi(t)\,dt$$
$$- 8 \sum_{\frac{x}{2} < m^k \leqq x} \psi\big((x - m^k)^{1/k}\big) + O(1)$$

und bei Verwendung von (27)

$$R_{2,k}(x) = 4\int_0^{x^{1/k}} (x - t^k)^{1/k}\,dt + \varrho_k(x^{1/k}) - 8 \sum_{\frac{x}{2} < m^k \leqq x} \psi\big((x - m^k)^{1/k}\big) + O(1).$$

Der Hilfssatz 6.11 gibt

$$R_{2,k}(x) = c_k x^{2/k} + \varrho_k(x^{1/k}) + O\big(x^{2/3k}(\log x)^{2/3}\big).$$

Bei Berücksichtigung von Hilfssatz 6.13 ergibt sich für $k = 2$ nochmals der Satz 6.26 und für $k > 2$ der Satz 6.28.

6.5.4. Das Teilerproblem und Verallgemeinerungen

Es wird eine Verbesserung der Abschätzung des Satzes 5.39 mit Hilfe der Vinogradovschen Methode gegeben.

Satz 6.29. *Für die Anzahl $D(x)$ der Gitterpunkte unterhalb und auf der Hyperbel $\xi\eta = x$ $(\xi > 0, \eta > 0)$ gilt*

$$D(x) = x \log x + (2C - 1)\,x + O\big(x^{1/3}(\log x)^{5/3}\big),$$

worin C die Eulersche Konstante bedeutet.

Beweis. Es gilt

$$D(x) = \sum_{1 \leqq nm \leqq x} 1 = 2 \sum_{1 \leqq n \leqq \sqrt{x}} \sum_{m \leqq \frac{x}{n}} 1 - \big[\sqrt{x}\big]^2$$
$$= 2 \sum_{1 \leqq n \leqq \sqrt{x}} \left[\frac{x}{n}\right] - \big[\sqrt{x}\big]^2$$
$$= 2 \sum_{1 \leqq n \leqq \sqrt{x}} \left\{\frac{x}{n} - \psi\left(\frac{x}{n}\right) - \frac{1}{2}\right\} - \left\{\sqrt{x} - \psi\big(\sqrt{x}\big) - \frac{1}{2}\right\}^2$$
$$= 2 \sum_{1 \leqq n \leqq \sqrt{x}} \frac{x}{n} - x + 2\sqrt{x}\,\psi\big(\sqrt{x}\big) - 2 \sum_{1 \leqq n \leqq \sqrt{x}} \psi\left(\frac{x}{n}\right) + O(1)$$
$$= x \log x + (2C - 1)\,x - 2 \sum_{1 \leqq n \leqq \sqrt{x}} \psi\left(\frac{x}{n}\right) + O(1).$$

Auf die verbleibende Summe

$$\sum_{1\leqq n\leqq\sqrt{x}} \psi\left(\frac{x}{n}\right) = \sum_{(59x)^{1/3}<n\leqq\sqrt{x}} \psi\left(\frac{x}{n}\right) + O(x^{1/3})$$

wenden wir Hilfssatz 6.12 an, indem wir dort $y = x$, $r = 1$, $A = (59x)^{1/3}$, $B = x$ setzen. Die Voraussetzung $A^3 > 58y$ ist somit erfüllt, und wir erhalten

$$\sum_{1\leqq n\leqq\sqrt{x}} \psi\left(\frac{x}{n}\right) = O\left(x^{1/3}(\log x)^{3/5}\right)$$

und damit die Behauptung des Satzes.

Als *Teilerproblem* bezeichnet man die Aufgabe, das Infimum, $\vartheta = \inf \beta$, in der Abschätzung

$$D(x) = x \log x + (2C - 1)\, x + O(x^{\beta})$$

zu bestimmen. Seinen historischen Ausgangspunkt hat dieses Problem bei P. G. L. Dirichlet gefunden, von dem nach Satz 5.39 $\vartheta \leqq \frac{1}{2}$ stammt. Auch hier läßt sich $\vartheta \geqq 0$ ganz leicht zeigen.

Satz 6.30. *Die Gleichung*

$$D(x) = x \log x + (2C - 1)\, x + o(\log x)$$

ist falsch.

Beweis. Wir nehmen an, die Gleichung sei richtig und bilden mit einer natürlichen Zahl n

$$\begin{aligned} 0 = D\left(n + \frac{1}{2}\right) - D(n) &= \left(n + \frac{1}{2}\right)\log\left(n + \frac{1}{2}\right) - n \log n + o(\log n) \\ &= \left(n + \frac{1}{2}\right)\log\left(1 + \frac{1}{2n}\right) + \frac{1}{2}\log n + o(\log n) \\ &= \frac{1}{2}\log n + o(\log n). \end{aligned}$$

Dies ist aber offensichtlich ein Widerspruch.

Die Entwicklung des Teilerproblems verlief weitgehend parallel zum Kreisproblem. G. F. Voronoi (1868—1908) zeigte 1903 $\vartheta \leqq \frac{1}{3}$, was 1917 I. M. Vinogradov elementar beweisen konnte, wie aus unserem Satz 6.29 ersichtlich wird. G. H. Hardy wies 1915 $\vartheta \geqq \frac{1}{4}$ nach, was H. E. Richert 1958 auch elementar gelang. J. G. van der Corput brach 1922 den klassischen Rekord $\vartheta \leqq \frac{1}{3}$ und erzielte $\vartheta \leqq \frac{33}{100}$. In den folgenden Jahren gab es zahlreiche Verbesserungen bis hin zu $\vartheta \leqq \frac{346}{1\,067}$ durch G. A. Kolesnik im Jahre 1973.

Mit Hilfe der Vinogradovschen Methode soll abschließend eine Verbesserung der Abschätzung von $D(a, b; x)$ des Satzes 5.40 hergeleitet werden.

Satz 6.31. *Für $1 \leqq a < b$ gilt*

$$D(a, b; x) = \zeta\left(\frac{b}{a}\right) x^{1/a} + \zeta\left(\frac{a}{b}\right) x^{1/b} + O\left(x^{\frac{1}{2a+b}} (\log x)^{2/3}\right).$$

Beweis. Aus dem Beweis zu Satz 5.40 übernehmen wir

$$D(a,b;x) = \sum_{1 \le n^a m^b \le x} 1 = \sum_{1 \le n^{a+b} \le x} \left\{ \left[\left(\frac{x}{n^b} \right)^{1/a} \right] + \left[\left(\frac{x}{n^a} \right)^{1/b} \right] \right\} - \left[x^{\frac{1}{a+b}} \right]^2 .$$

Mit $\psi(y) = y - [y] - \frac{1}{2}$ ist

$$D(a,b;x) = \sum_{1 \le n^{a+b} \le x} \left\{ \left(\frac{x}{n^b} \right)^{1/a} + \left(\frac{x}{n^a} \right)^{1/b} \right\} - x^{\frac{2}{a+b}} + 2x^{\frac{1}{a+b}} \psi\left(x^{\frac{1}{a+b}} \right)$$
$$- \sum_{1 \le n^{a+b} \le x} \left\{ \psi\left(\left(\frac{x}{n^b} \right)^{1/a} \right) + \psi\left(\left(\frac{x}{n^a} \right)^{1/b} \right) \right\} + O(1).$$

Entwickeln wir die erste Summe mit Hilfe der Formel (10) aus Kapitel 5, so erhalten wir

$$D(a,b;x) = \zeta\left(\frac{b}{a} \right) x^{1/a} + \zeta\left(\frac{a}{b} \right) x^{1/b} + \Delta(a,b;x)$$

mit

$$\Delta(a,b;x) = - \sum_{1 \le n^{a+b} \le x} \left\{ \psi\left(\left(\frac{x}{n^b} \right)^{1/a} \right) + \psi\left(\left(\frac{x}{n^a} \right)^{1/b} \right) \right\} + O(1). \tag{28}$$

Für den ersten Teil der Summe bilden wir

$$\sum_{1 \le n^{a+b} \le x} \psi\left(\left(\frac{x}{n^b} \right)^{1/a} \right) = \sum_{A < n \le B} \psi\left(\left(\frac{x}{n^b} \right)^{1/a} \right) + O\left(x^{\frac{1}{2a+b}} \right)$$

und wenden darauf den Hilfssatz 6.12 mit

$$y = x^{1/a}, \quad r = \frac{b}{a} > 1, \quad A = \left(29 \frac{b}{a} \left(\frac{b}{a} + 1 \right) x^{1/a} \right)^{\frac{a}{2a+b}}, \quad B = x^{\frac{1}{a+b}}$$

an. Wir erhalten

$$\sum_{1 \le n^{a+b} \le x} \psi\left(\left(\frac{x}{n^b} \right)^{1/a} \right) = O\left(x^{\frac{2}{3(a+b)}} (\log x)^{2/3} \right) + O\left(x^{\frac{1}{2a+b}} (\log x)^{2/3} \right)$$
$$= O\left(x^{\frac{1}{2a+b}} (\log x)^{2/3} \right). \tag{29}$$

Für den zweiten Teil der Summe (28) bilden wir analog

$$\sum_{1 \le n^{a+b} \le x} \psi\left(\left(\frac{x}{n^a} \right)^{1/b} \right) = \sum_{A < n \le B} \psi\left(\left(\frac{x}{n^a} \right)^{1/b} \right) + O\left(x^{\frac{1}{a+2b}} \right),$$

indem wir jetzt entsprechend Hilfssatz 6.12

$$y = x^{1/b}, \quad r = \frac{a}{b} < 1, \quad A = \left(29 \frac{a}{b} \left(\frac{a}{b} + 1 \right) x^{1/b} \right)^{\frac{b}{a+2b}}, \quad B = x^{\frac{1}{a+b}}$$

setzen. Es ergibt sich

$$\sum_{1\leqq n^{a+b}\leqq x}\psi\left(\left(\frac{x}{n^a}\right)^{1/b}\right)=O\left(x^{\frac{2}{3(a+b)}}(\log x)^{2/3}\right)+O\left(x^{\frac{1}{a+2b}}\right)$$

$$=O\left(x^{\frac{2}{3(a+b)}}(\log x)^{2/3}\right). \tag{30}$$

Setzt man (29) und (30) in (28) ein, so folgt wegen $\frac{1}{2a+b}>\frac{2}{3(a+b)}$ die Behauptung.

6.6. Gitterpunkte in mehrdimensionalen Kugeln

Wir betrachten die Anzahl

$$R_k(x)=\sum_{n_1^2+n_2^2+\cdots+n_k^2\leqq x}1$$

der Gitterpunkte in einer k-dimensionalen Kugel ($k\geqq 2$). In Hinblick auf Satz 6.24 werden wir auch hier erwarten können, daß sich die Gitterpunktanzahl in erster Näherung durch das Volumen der Kugel approximieren läßt. Bezeichnet V_k das Volumen der k-dimensionalen Einheitskugel, so läßt sich V_k über $V_1=2$ durch die Rekursionsformel

$$V_k=V_{k-1}\int_{-1}^{+1}(1-t^2)^{\frac{k-1}{2}}\,dt$$

berechnen. Dabei ergibt sich insbesondere $V_2=\pi$, $V_3=\frac{4}{3}\pi$, $V_4=\frac{1}{2}\pi^2$. In Verallgemeinerung von Satz 5.37 erhalten wir:

Satz 6.32. *Es ist*

$$R_k(x)=V_kx^{k/2}+O\left(x^{\frac{k-1}{2}}\right).$$

Beweis. Für $k=2$ ist die Aussage nach Satz 5.37 richtig. Nehmen wir ihre Richtigkeit für $k-1$ an und schließen auf k.

$$R_k(x)=\sum_{n^2+n_1^2+\cdots+n_{k-1}^2\leqq x}1=\sum_{n^2\leqq x}R_{k-1}(x-n^2)$$

$$=\sum_{n^2\leqq x}\left\{V_{k-1}(x-n^2)^{\frac{k-1}{2}}+O\left((x-n^2)^{\frac{k-2}{2}}\right)\right\}.$$

Nach der Euler-Maclaurinschen Summenformel ist

$$R_k(x)=V_{k-1}\int_{-\sqrt{x}}^{\sqrt{x}}(x-t^2)^{\frac{k-1}{2}}\,dt-(k-1)\,V_{k-1}\int_{-\sqrt{x}}^{\sqrt{x}}\psi(t)\,t(x-t^2)^{\frac{k-3}{2}}\,dt+O\left(x^{\frac{k-1}{2}}\right)$$

$$=V_kx^{k/2}+O\left(x^{\frac{k-1}{2}}\right).$$

Im Unterschied zu allen bisherigen Restabschätzungen können wir die Abschätzung des Satzes 6.32 für $k \geqq 4$ erheblich verbessern. Das liegt an der besonderen Struktur der zahlentheoretischen Funktion $r_4(n)$ in

$$R_4(x) = \sum_{n \leqq x} r_4(n),$$

die sich nach Satz 6.17 durch Teilerfunktionen darstellen läßt.

Satz 6.33. *Für $k \geqq 4$ gilt*

$$R_k(x) = V_k x^{k/2} + O\left(x^{\frac{k}{2}-1} \log x\right). \tag{31}$$

Beweis. Wir behandeln zunächst den Fall $k = 4$. Nach Satz 6.17 ist

$$R_4(x) = \sum_{n \leqq x} r_4(n) = 1 + 8 \sum_{1 \leqq n \leqq x} \sigma(n) - 32 \sum_{1 \leqq n \leqq x/4} \sigma(n).$$

Nun ist nach Satz 5.40

$$\sum_{1 \leqq n \leqq x} \sigma(n) = \frac{\pi^2}{12} x^2 + O(x \log x)$$

und damit

$$R_4(x) = \frac{\pi^2}{2} x^2 + O(x \log x).$$

Ähnlich wie im Beweis des vorigen Satzes schließen wir durch Induktion auf beliebiges k. Der Satz sei für $k - 1$ als richtig angenommen, so ist

$$\begin{aligned} R_k(x) &= \sum_{n^2 \leqq x} R_{k-1}(x - n^2) \\ &= \sum_{n^2 \leqq x} \left\{ V_{k-1}(x - n^2)^{\frac{k-1}{2}} + O\left(x^{\frac{k-3}{2}} \log x\right) \right\} \\ &= V_k x^{k/2} - 2(k-1)\, V_{k-1} \int_0^{\sqrt{x}} \psi(t)\, t (x - t^2)^{\frac{k-1}{2}-1}\, dt + O\left(x^{\frac{k}{2}-1} \log x\right) \\ &= V_k x^{k/2} + 2(k-1)\, V_{k-1} x^{\frac{k}{2}-1} \int_0^1 \psi_1(\sqrt{x}\, t) \frac{d}{dt} \left\{ t(1-t^2)^{\frac{k-1}{2}-1} \right\} dt \\ &\quad + O\left(x^{\frac{k}{2}-1} \log x\right) = V_k x^{k/2} + O\left(x^{\frac{k}{2}-1} \log x\right). \end{aligned}$$

Der Satz 6.33 ist insofern bemerkenswert, daß die Abschätzung bis auf den logarithmischen Faktor genau ist. Das heißt, der Exponent $\frac{k}{2} - 1$ im O-Glied kann durch keinen kleineren ersetzt werden. Das harmoniert mit dem Satz 6.27 und kann ebenso einfach nachgewiesen werden.

Satz 6.34. *Die Gleichung*

$$R_k(x) = V_k x^{k/2} + o\left(x^{\frac{k}{2}-1}\right) \tag{32}$$

ist falsch.

Beweis. Wir nehmen an, die Gleichung (32) ist richtig. Für natürliche Zahlen n ist dann

$$O = R_k\left(n + \frac{1}{2}\right) - R_k(n) = V_k\left\{\left(n + \frac{1}{2}\right)^{k/2} - n^{k/2}\right\} + o\left(n^{\frac{k}{2}-1}\right)$$

$$= V_k \frac{k}{4} n^{\frac{k}{2}-1} + o\left(n^{\frac{k}{2}-1}\right),$$

was einen offensichtlichen Widerspruch darstellt.

In (31) kann man für $k > 4$ in der Restabschätzung den logarithmischen Faktor noch beseitigen, so daß man mit

$$R_k(x) = V_k x^{k/2} + O\left(x^{\frac{k}{2}-1}\right)$$

eine endgültige, nicht mehr zu verbessernde Abschätzung erhält. Es soll dieses Resultat nicht vorgestellt werden, sondern nur darauf hingewiesen werden, daß für $k = 4$ eine andere Situation vorliegt.

Satz 7.34. *Die Gleichung*

$$R_4(x) = V_4 x^2 + o(x \log\log x) \tag{33}$$

ist falsch.

Beweis. Nach Satz 5.26 gibt es unendlich viele natürliche Zahlen n_ν, für die

$$\sigma(n_\nu) = o(n_\nu \log\log n_\nu)$$

falsch ist. Es ist aber nicht nötig, die damals verwendete Zahlenfolge $\{n_\nu\}$ zu betrachten. Wir können es uns etwas einfacher machen. Wir betrachten für $\nu = 2, 3, \ldots$ die Zahlen

$$n_\nu = 1 \cdot 3 \cdot 5 \cdots (2\nu - 1) = \frac{(2\nu)!}{2^\nu \nu!}.$$

Nach der Stirlingschen Formel ist

$$\log n_\nu = \log (2\nu)! - \nu \log 2 - \log \nu!$$

$$= \nu \log \nu + O(\nu)$$

und daher

$$\log\log n_\nu \sim \log \nu \qquad (\nu \to \infty).$$

Hieraus und aus

$$\sigma(n_\nu) = \sum_{t \mid n_\nu} t \geqq \sum_{\varrho=1}^{\nu} \frac{n_\nu}{2\varrho - 1} = n_\nu \sum_{\varrho=1}^{2\nu} \frac{1}{\varrho} - n_\nu \sum_{\varrho=1}^{\nu} \frac{1}{2\varrho}$$

$$= n_\nu \left\{\log (2\nu) - \frac{1}{2} \log \nu + O(1)\right\}$$

$$= \frac{n_\nu}{2} \log \nu + O(n_\nu)$$

folgt, daß jedenfalls

$$\sigma(n_\nu) = o(n_\nu \log\log n_\nu)$$

falsch ist. Nach Satz 6.17 ist $r_4(n_\nu) = 8\sigma(n_\nu)$. Also ist auch

$$r_4(n_\nu) = o(n_\nu \log\log n_\nu) \tag{34}$$

falsch. Nehmen wir nun im Gegensatz zur Behauptung die Richtigkeit von (33) an. Dann bildet aber

$$r_4(n_\nu) = R_4(n_\nu) - R_4(n_\nu - 1) = o(n_\nu \log\log n_\nu)$$

einen offensichtlichen Widerspruch zu (34).

6.7. Aufgaben

1. Es sind die sämtlichen Gitterpunkte auf der Parabel $9x^2 + 42xy + 49y^2 - 5y - 4 = 0$ zu bestimmen.
2. Man beweise: Unter allen Primzahlen gestatten genau diejenigen, für die
   a) $p \equiv 1,3$ (8) gilt, die Darstellung $p = x^2 + 2y^2$,
   b) $p \equiv 1,9$ (14) gilt, die Darstellung $p = x^2 + 7y^2$, wobei x und y natürliche Zahlen sind.
3. Es ist zu zeigen, daß 2713 eine Primzahl ist.
5. Der Zusammenhang zwischen den Darstellungen einer Primzahl p als Summe von zwei Quadraten natürlicher Zahlen mit den Lösungen der Kongruenz $z^2 \equiv -1 \ (p)$ ist zur Lösung von $z^2 \equiv -1$ (2713) zu benutzen.
5. Besitzt die Gleichung $x^2 - 11y^2 = -1$ Lösungen in ganzen Zahlen?
6. Es sind die Lösungsklassen von a) $u^2 - 11v^2 = 5$, b) $u^2 - 11v^2 = -7$ anzugeben.
7. Die Anzahl der Darstellungen einer ganzen Zahl als Summe von zwei Kuben ganzer Zahlen ist endlich. — W. Sierpiński.
8. Keine ganze Zahl der Form $9k \pm 4$ ist Summe von drei Kuben ganzer Zahlen. — W. Sierpiński.
9. Welche Primzahlen p sind a) Summe, b) Differenz von zwei Kuben natürlicher Zahlen.
10. Es sind alle rationalen Punkte auf den Kurven $x^2 \pm 3y^2 = 7$ zu bestimmen.
11. Bilden die Zahlen a, b, c ein Pythagoräisches Zahlentripel, so ist stets $60 \mid abc$.
12. Man ermittle alle gleichschenkligen Dreiecke, deren Seitenlängen und Flächeninhalte ganze Zahlen sind.
13. Es sind alle natürlichen Zahlen x, y, z mit $(x, y, z) = 1$ anzugeben, die der Gleicnung $x^2 + 2y^2 = z^2$ genügen.
14. Man zeige, daß die Gleichung $x^4 + 4y^4 = z^2$ mit $(x, y, z) = 1$ keine Lösungen in natürlichen Zahlen besitzt.
15. Man zeige, daß die Gleichung $x^4 + y^4 + z^4 = w^2$ unendlich viele Lösungen in natürlichen Zahlen x, y, z, w mit $(x, y, z) = 1$ besitzt.

    Hinweis: Man benutze die aus $a^2 + b^2 = c^2$ folgende Identität $(ab)^4 + (ac)^4 + (bc)^4 = (c^4 - a^2b^2)^2$. — W. Sierpiński.
16. Für jede natürliche Zahl n existiert in der Ebene ein Kreis, der in seinem Inneren genau n Gitterpunkte enthält.

    Hinweis: Auf der Peripherie eines jeden Kreises mit dem Mittelpunkt $\left(\sqrt{2}, \frac{1}{3}\right)$ liegt höchstens ein Gitterpunkt. — H. Steinhaus.
17. Jede Kugel mit dem Mittelpunkt $(\sqrt{2}, \sqrt{3}, \sqrt{5})$ geht durch höchstens einen Gitterpunkt. — W. Sierpiński.
18. Der Kreis $\left(x - \sqrt{2}\right)^2 + \left(y - \sqrt{2}\right)^2 = 4$ enthält genau einen rationalen Punkt.
19. Der Kreis $x^2 + \left(y - \sqrt{2}\right)^2 = 3$ enthält genau zwei rationale Punkte.
20. Jeder Kreis mit drei rationalen Punkten enthält unendlich viele rationale Punkte.
    Hinweis: Jeder Kreis mit drei rationalen Punkten hat einen rationalen Mittelpunkt. — W. Sierpiński.

7. Partitionen

Im dritten Kapitel waren wir bereits auf den Begriff der Partition gestoßen. Es handelt sich um die Zerlegung einer natürlichen Zahl in eine Summe von natürlichen Zahlen. Hier geht es vornehmlich um die Abschätzung der Anzahl solcher Zerlegungen. Dabei ziehen wir auch Zerlegungen in eine beschränkte Anzahl von Summanden in Betracht. Abschließend wenden wir die Ergebnisse, wie bereits in Kapitel 3 ebenfalls angedeutet, auf die Anzahl der nicht-isomorphen abelschen Gruppen n-ter Ordnung an.

7.1. Elementare Eigenschaften

Definition 7.1. Für $k \in \mathbf{N}$ bezeichne $P_k(n)$ die *Anzahl der Partitionen* der natürlichen Zahl n *in höchstens* k *Summanden* natürlicher Zahlen. Ferner sei $P_k(0) = 1$ gesetzt.

Es ist natürlich $P_1(n) = 1$. $P_2(n)$ ist gleich der Anzahl der Darstellungen von n in der Form $n = n_1 + n_2$ mit $n_1 \geqq n_2 \geqq 0$. Wir wollen $P_2(n)$ berechnen.

$$P_2(n) = \sum_{\substack{n_1+n_2=n \\ n_1 \geqq n_2}} 1 = \frac{1}{2} \sum_{n_1+n_2=n} 1 + \frac{1}{2} \sum_{\substack{n_1+n_2=n \\ n_1=n_2}} 1$$

$$= \frac{n+1}{2} + \begin{cases} \frac{1}{2} & \text{für} \quad n \equiv 0 \quad (2), \\ 0 & \text{für} \quad n \equiv 1 \quad (2). \end{cases}$$

Damit ergibt sich

$$P_2(n) = \left[\frac{n}{2}\right] + 1. \tag{1}$$

Die Berechnung von $P_k(n)$ für $k \geqq 3$ bringt sehr schnell erhebliche rechentechnische Probleme mit sich. Wir leiten für $P_k(n)$ eine Rekursionsformel her und benutzen diese für Abschätzungen. $P_k(n)$ gibt die Anzahl der Darstellungen von n in der Form

$$n = n_1 + n_2 + \cdots + n_k, \qquad n_1 \geqq n_2 \geqq \cdots \geqq n_k \geqq 0$$

an. Dies kann man auch in die Gestalt

$$n = (n_1 - n_2) + 2(n_2 - n_3) + \cdots + kn_k$$
$$= m_1 + 2m_2 + \cdots + km_k, \qquad m_1, m_2, \ldots, m_k \geqq 0$$

bringen. Mit $|z| < 1$ bilden wir hieraus ableitend die erzeugende Funktion

$$F_k(z) = \sum_{n=0}^{\infty} P_k(n) z^n = \sum_{m_1=0}^{\infty} \cdots \sum_{m_k=0}^{\infty} z^{m_1+2m_2+\cdots+km_k} = \prod_{\nu=1}^{k} (1 - z^\nu)^{-1}. \tag{2}$$

Diese Funktion hat für $k \geqq 2$ die Eigenschaft

$$(1 - z^k) F_k(z) = F_{k-1}(z).$$

Andererseits gilt

$$(1 - z^k) F_k(z) = \sum_{n=0}^{\infty} P_k(n) (1 - z^k) z^n = \sum_{n=0}^{\infty} P_k(n) z^n - \sum_{n=k}^{\infty} P_k(n - k) z^n.$$

Vereinbaren wir noch $P_k(m) = 0$ für $m < 0$, so haben wir

$$(1 - z^k) F_k(z) = \sum_{n=0}^{\infty} \{P_k(n) - P_k(n - k)\} z^n = F_{k-1}(z) = \sum_{n=0}^{\infty} P_{k-1}(n) z^n.$$

Durch Koeffizientenvergleich ergibt sich

$$P_k(n) - P_k(n - k) = P_{k-1}(n).$$

Damit haben wir für $P_k(n)$ eine Differenzengleichung, die die Funktion rekursiv zu berechnen gestattet. Wir haben also bewiesen:

Satz 7.1. *Durch die Differenzengleichung*

$$P_k(n) = P_k(n - k) + P_{k-1}(n)$$

mit $P_k(n) = 0$ *für* $n < 0$ *und* $P_1(n) = 1$ *für* $n \geqq 0$ *ist* $P_k(n)$ *für* $k \geqq 2$ *rekursiv bestimmt.*

Wir benutzen diesen Satz zur Abschätzung von $P_3(n)$. Nach (1) ist

$$P_3(n) = P_3(n - 3) + \left[\frac{n}{2}\right] + 1 \leqq P_3(n - 3) + \frac{n + 2}{2}$$

$$\leqq \sum_{0 \leqq \nu \leqq n/3} \frac{n + 2 - 3\nu}{2}$$

$$= \left(\frac{n}{2} + 1\right)\left(\left[\frac{n}{3}\right] + 1\right) - \frac{3}{4}\left[\frac{n}{3}\right]\left(\left[\frac{n}{3}\right] + 1\right)$$

$$< \left(\frac{n}{2} + 1\right)\left(\frac{n}{3} + 1\right) - \frac{3}{4}\left(\frac{n}{3} - 1\right)\frac{n}{3} = \frac{n^2}{12} + \frac{13n}{12} + 1.$$

Entsprechend ist

$$P_3(n) > P_3(n-3) + \frac{n}{2} > \frac{n}{2}\left(\left[\frac{n}{3}\right]+1\right) - \frac{3}{4}\left[\frac{n}{3}\right]\left(\left[\frac{n}{3}\right]+1\right)$$

$$> \frac{n^2}{6} - \frac{3}{4}\frac{n}{3}\left(\frac{n}{3}+1\right) = \frac{n^2}{12} - \frac{n}{4}.$$

Zusammenfassend haben wir die Abschätzung

$$\frac{n^2}{12} - \frac{n}{4} < P_3(n) < \frac{n^2}{12} + \frac{13n}{12} + 1.$$

Wir beweisen jetzt mit Hilfe der erzeugenden Funktion (2) eine Rekursionsformel für $P_k(n)$, bei der k fest bleibt.

Satz 7.2. *Es bezeichne*

$$\sigma(n;k) = \sum_{\substack{t\mid n \\ t\leqq k}} t,$$

dann gilt

$$nP_k(n) = \sum_{\nu=1}^{n} \sigma(\nu;k)\, P_k(n-\nu).$$

Beweis. Aus (2) folgt

$$\frac{F_k'(z)}{F_k(z)} = \frac{d}{dz}\log F_k(z) = \sum_{\nu=1}^{k} \frac{\nu z^{\nu-1}}{1-z^\nu} = \sum_{\nu=1}^{k}\sum_{m=1}^{\infty} \nu z^{\nu m-1} = \sum_{n=1}^{\infty}\left(\sum_{\substack{\nu m=n \\ \nu\leqq k}} \nu\right) z^{n-1},$$

$$F_k'(z) = F_k(z)\sum_{n=1}^{\infty} \sigma(n;k)\, z^{n-1},$$

$$\sum_{n=1}^{\infty} nP_k(n)\, z^{n-1} = \sum_{m=0}^{\infty}\sum_{\nu=1}^{\infty} \sigma(\nu;k)\, P_k(m)\, z^{\nu+m-1}.$$

Der Vergleich der Koeffizienten ergibt die Behauptung.

Jetzt wenden wir uns der in Definition 3.2 gegebenen Funktion $P(n)$, der Anzahl der Partitionen von n in eine unbeschränkte Anzahl von Summanden, zu. Wir legen auch hier $P(0) = 1$ fest. Es ist stets $P_k(n) \leqq P(n)$, $P_k(n) = P(n)$ für $n \leqq k$, und für $k \to \infty$ gilt $P_k(n) \to P(n)$. Ermitteln wir eine erzeugende Funktion für $P(n)$. Für $0 < z < 1$ ist

$$\sum_{n=0}^{k} P(n)\, z^n = \sum_{n=0}^{k} P_k(n)\, z^n < \sum_{n=0}^{\infty} P_k(n)\, z^n = \prod_{\nu=1}^{k} (1-z^\nu)^{-1} < \prod_{\nu=1}^{\infty} (1-z^\nu)^{-1}.$$

Daher konvergiert

$$F(z) = \sum_{n=0}^{\infty} P(n)\, z^n$$

für $|z| < 1$. Wegen

$$\sum_{n=0}^{\infty} P_k(n)\, z^n < \sum_{n=0}^{\infty} P(n)\, z^n$$

wieder für $0 < z < 1$ konvergiert die links stehende Summe gleichmäßig in k. Deshalb ist

$$F(z) = \sum_{n=0}^{\infty} P(n)\, z^n = \lim_{k\to\infty} \sum_{n=0}^{\infty} P_k(n)\, z^n = \lim_{k\to\infty} \prod_{\nu=1}^{k} (1 - z^\nu)^{-1},$$

$$F(z) = \prod_{\nu=1}^{\infty} (1 - z^\nu)^{-1}. \tag{3}$$

Mit dieser erzeugenden Funktion bereitet die Übertragung des Satzes 7.2 keine Schwierigkeiten.

Satz 7.3. *Es gilt*

$$nP(n) = \sum_{\nu=1}^{n} \sigma(\nu)\, P(n - \nu).$$

Beweis.

$$\frac{F'(z)}{F(z)} = \frac{d}{dz} \log F(z) = \sum_{\nu=1}^{\infty} \frac{\nu z^{\nu-1}}{1 - z^\nu} = \sum_{\nu=1}^{\infty} \sum_{m=1}^{\infty} \nu z^{\nu m - 1}$$

$$= \sum_{n=1}^{\infty} \Big(\sum_{\nu m = n} \nu \Big) z^{n-1},$$

$$F'(z) = F(z) \sum_{n=1}^{\infty} \sigma(n)\, z^{n-1},$$

$$\sum_{n=1}^{\infty} n\, P(n)\, z^{n-1} = \sum_{m=0}^{\infty} \sum_{\nu=1}^{\infty} \sigma(\nu)\, P(m)\, z^{\nu+m-1}.$$

Aus dem Koeffizientenvergleich folgt die Behauptung.

Wir leiten jetzt noch eine Beziehung zwischen $P(n)$ und $P_k(n)$ her und bereiten dies mit einem Hilfssatz vor.

Hilfssatz 7.1. *Es seien x, z reelle Zahlen mit $|z| < 1$. Dann ist*

$$\prod_{m=1}^{\infty} (1 - xz^m)^{-1} = 1 + \sum_{n=1}^{\infty} (xz)^n \prod_{\nu=1}^{n} (1 - z^\nu)^{-1}.$$

Beweis. Für

$$F(x, z) = \prod_{m=1}^{\infty} (1 - xz^m)^{-1}$$

besteht die Funktionalgleichung

$$F(xz, z) = (1 - xz)\, F(x, z).$$

Verwenden wir sie in dem Ansatz

$$F(x, z) = \sum_{n=0}^{\infty} a_n x^n, \qquad a_0 = 1,$$

so erhalten wir

$$\sum_{n=0}^{\infty} a_n (xz)^n = (1 - xz) \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} a_n x^n - \sum_{n=1}^{\infty} a_{n-1} z x^n$$

und durch Koeffizientenvergleich für $n \geqq 1$

$$a_n z^n = a_n - a_{n-1} z.$$

Mit $a_0 = 1$ errechnet sich hieraus

$$a_n = z^n \prod_{\nu=1}^{n} (1 - z^\nu)^{-1}.$$

Dies gibt die Behauptung.

Satz 7.4. *Für $n \geqq 1$ gilt*

$$P(n) = \sum_{k=1}^{n} P_k(n - k).$$

Beweis. Wir setzen in der Formel des Hilfssatzes $x = 1$ und bekommen aus

$$\prod_{\nu=1}^{\infty} (1 - z^\nu)^{-1} = 1 + \sum_{k=1}^{\infty} z^k \prod_{\mu=1}^{k} (1 - z^\mu)^{-1}$$

mit (2) und (3)

$$\sum_{n=0}^{\infty} P(n) z^n = 1 + \sum_{k=1}^{\infty} \sum_{\nu=0}^{\infty} P_k(\nu) z^{\nu+k}.$$

Koeffizientenvergleich ergibt die Behauptung.

7.2. Abschätzungen und asymptotische Darstellungen

Wir beginnen mit Abschätzungen von $P(n)$.

Satz 7.5 (KRÄTZEL). *Für alle natürlichen Zahlen n ist*

$$P(n) \leqq 5^{n/4},$$

wobei das Gleichheitszeichen nur für $n = 4$ gilt.

Beweis. Mit Hilfe der Tabelle in 3.1 bestätigt man die Aussage für $1 \leqq n \leqq 11$. Jetzt setzen wir den Beweis durch Induktion fort. Wir nehmen die Richtigkeit für alle Zahlen kleiner als n an. Nach Satz 7.3 ist dann

$$P(n) = \frac{1}{n} \sum_{\nu=1}^{n} \sigma(\nu) P(n - \nu) < \frac{1}{n} \sum_{\nu=1}^{n} \sigma(\nu) 5^{\frac{n-\nu}{4}},$$

und mit

$$\sigma(\nu) = \sum_{\mu m = \nu} \mu$$

ergibt sich

$$P(n) < 5^{n/4} \frac{1}{n} \sum_{m=1}^{\infty} \sum_{\mu=1}^{\infty} \mu 5^{-\mu m/4} = 5^{n/4} \cdot \frac{1}{n} \cdot \sum_{m=1}^{\infty} (5^{m/8} - 5^{-m/8})^{-2}.$$

Aus $e^x - e^{-x} \geqq 2x$ für $x \geqq 0$ folgt weiter

$$P(n) < 5^{n/4} \cdot \frac{1}{n} \cdot \sum_{m=1}^{\infty} \frac{16}{m^2 (\log 5)^2} = 5^{n/4} \cdot \frac{1}{n} \cdot \frac{8\pi^2}{3(\log 5)^2} < 5^{n/4}$$

für $n \geqq 11$.

Diese Abschätzung ist für kleine n zwar recht gut, doch können wir sie für große n durch eine bessere ersetzen.

Satz 7.6. *Es gilt*

$$P(n) < \frac{\pi}{\sqrt{6n}} e^{\pi\sqrt{2n/3}}.$$

Beweis. Wir benutzen die erzeugende Funktion (3)

$$F(z) = \sum_{m=0}^{\infty} P(m) z^m = \prod_{\nu=1}^{\infty} (1 - z^\nu)^{-1}$$

mit $0 < z < 1$. Wegen $P(m) \geqq 0$ und $P(m) \geqq P(n)$ für $m \geqq n$ ist

$$F(z) \geqq \sum_{m=n}^{\infty} P(n) z^m = P(n) \frac{z^n}{1 - z},$$

und die Ungleichung

$$P(n) \leqq \frac{1 - z}{z^n} \prod_{\nu=1}^{\infty} (1 - z^\nu)^{-1}$$

gilt für alle z mit $0 < z < 1$. Es kommt darauf an, z in diesem Intervall so auszuwählen, daß die rechte Seite möglichst klein wird. Durch Logarithmieren erhalten wir

$$\begin{aligned} \log P(n) &\leqq \log (1 - z) - n \log z - \sum_{\nu=1}^{\infty} \log (1 - z^\nu) \\ &= \log (1 - z) - n \log z + \sum_{\nu=1}^{\infty} \sum_{m=1}^{\infty} \frac{z^{\nu m}}{m} \\ &= \log (1 - z) - n \log z + \sum_{m=1}^{\infty} \frac{1}{m} \frac{z^m}{1 - z^m}. \end{aligned}$$

Aus

$$\frac{1 - z^m}{1 - z} = 1 + z + z^2 + \cdots + z^{m-1} > m z^{m-1}$$

folgt

$$\log P(n) < \log(1-z) - n\log z + \frac{z}{1-z}\sum_{m=1}^{\infty}\frac{1}{m^2}$$

$$= \log(1-z) - n\log z + \frac{\pi^2}{6}\frac{z}{1-z}.$$

Setzen wir noch $z = \dfrac{1}{1+x}$ mit $x > 0$, so erhalten wir

$$\log P(n) < \log\frac{x}{1+x} + n\log(1+x) + \frac{\pi^2}{6}\cdot\frac{1}{x}$$

$$< \log\frac{x}{1+x} + nx + \frac{\pi^2}{6}\cdot\frac{1}{x}.$$

Das Minimum von

$$nx + \frac{\pi^2}{6}\cdot\frac{1}{x}$$

liegt bei $x = \dfrac{\pi}{\sqrt{6n}}$. Für diesen Wert ist

$$\log P(n) < -\log\left(1 + \frac{\sqrt{6n}}{\pi}\right) + \pi\sqrt{\frac{2}{3}n}$$

und

$$P(n) < \left(1 + \frac{\sqrt{6n}}{\pi}\right)^{-1} e^{\pi\sqrt{2n/3}} < \frac{\pi}{\sqrt{6n}}\, e^{\pi\sqrt{2n/3}}.$$

Anstelle dieser Abschätzung zeigten G. H. Hardy und S. Ramanujan bereits 1918 die asymptotische Darstellung für n

$$P(n) \sim \frac{1}{4n\sqrt{3}}\, e^{\pi\sqrt{2n/3}}.$$

H. Rademacher konnte die Hardy-Ramanujansche Methode so verfeinern, daß er 1937 eine explizite Darstellung von $P(n)$ in Gestalt einer unendlichen Reihe erreichte. P. Erdös bewies 1942 auf elementarem Wege

$$P(n) \sim \frac{C}{n}\, e^{\pi\sqrt{2/3n}}, \qquad C > 0.$$

D. Newman zeigte 1951 ebenfalls elementar $C = \dfrac{1}{4\sqrt{3}}$.

Analog kann man mit Hilfe der erzeugenden Funktion (2) eine Abschätzung für $P_k(n)$ gewinnen. Wir werden die Rechnung nicht durchführen, sondern gleich eine bessere Abschätzung, die 1942 H. Gupta angab, herleiten.

Satz 7.7 (Gupta). *Für alle $n \geqq 1$, $k \geqq 1$ gilt*

$$\frac{1}{k!}\binom{n+k-1}{k-1} \leqq P_k(n) \leqq \frac{1}{k!}\binom{n+k+\dfrac{k(k-1)}{2}}{k-1}.$$

Beweis. Für $k = 1$ ist die Aussage offensichtlich richtig. Wir setzen den Beweis durch Induktion nach k fort und nehmen die Richtigkeit für alle Zahlen kleiner als k an. Nach Satz 7.1 ist

$$\sum_{\nu=0}^{n} P_k(\nu) = \sum_{\nu=0}^{n} P_k(\nu - k) + \sum_{\nu=0}^{n} P_{k-1}(\nu),$$

$$\sum_{\nu=n-k+1}^{n} P_k(\nu) = \sum_{\nu=0}^{n} P_{k-1}(\nu). \tag{4}$$

Für die Abschätzung nach unten benutzen wir

$$\sum_{\nu=n-k+1}^{n} P_k(\nu) \leqq k P_k(n),$$

so daß aus (4)

$$P_k(n) \geqq \frac{1}{k} \sum_{\nu=0}^{n} P_{k-1}(\nu) \geqq \frac{1}{k!} \sum_{\nu=0}^{n} \binom{\nu + k - 2}{k - 2} = \frac{1}{k!} \binom{n + k - 1}{k - 1}$$

folgt. Für die Abschätzung nach oben benötigen wir

$$\sum_{\nu=n-k+1}^{n} P_k(\nu) \geqq k P_k(n - k + 1),$$

so daß wir aus (4) die Abschätzung

$$P_k(n) \leqq \frac{1}{k} \sum_{\nu=0}^{n+k-1} P_{k-1}(\nu) \leqq \frac{1}{k!} \sum_{\nu=0}^{n+k-1} \binom{\nu + k - 1 + \frac{(k-1)(k-2)}{2}}{k - 2}$$

$$= \frac{1}{k!} \sum_{\mu=1+\frac{(k-1)(k-2)}{2}}^{n+k+\frac{(k-1)(k-2)}{2}} \binom{\mu + k - 2}{k - 2} \leqq \frac{1}{k!} \binom{n + k + \frac{k(k-1)}{2}}{k - 1}$$

erhalten.

Aus diesem Satz läßt sich für das asymptotische Verhalten von $P_k(n)$ eine wichtige Folgerung ziehen.

Satz 7.8 (Erdös/Lehner). *Für $n \to \infty$ ist gleichmäßig in $k = o(n^{1/3})$*

$$P_k(n) \sim \frac{n^{k-1}}{k!(k-1)!}.$$

Bemerkung. Dieses Ergebnis erzielten P. Erdös und J. Lehner bereits 1941. Im Jahre 1951 zeigt G. Szekeres die Gültigkeit der asymptotischen Darstellung sogar für $k = o\left(\sqrt{n}\right)$.

Beweis. Betrachten wir zunächst die linke Seite der Ungleichung des Satzes 7.7. Es ist

$$\frac{1}{k!} \binom{n + k - 1}{k - 1} = \frac{1}{k!(k-1)!} \cdot \frac{(n + k - 1)!}{n!}.$$

Mit Hilfe der Stirlingschen Formel werden wir

$$\frac{(n+k-1)!}{n!} \sim n^{k-1}$$

für $k = o(\sqrt{n})$ zeigen. Es ergibt sich

$$\frac{(n+k-1)!}{n^{k-1}n!} \sim \frac{(n+k-1)^{n+k-1}}{n^{n+k-1}} \sqrt{\frac{n+k-1}{n}}\, e^{1-k}$$

$$\sim \left(1+\frac{k-1}{n}\right)^{n+k-1} e^{1-k} = e^{1-k+(n+k-1)\log\left(1+\frac{k-1}{n}\right)}$$

$$= e^{O(k^2/n)} \sim 1.$$

Für $k = o(\sqrt{n})$ ist daher

$$\frac{1}{k!}\binom{n+k-1}{k-1} \sim \frac{n^{k-1}}{k!(k-1)!}. \tag{5}$$

Für die rechte Seite der Ungleichung des Satzes 7.7 ist mit $c = \frac{k(k-1)}{2}$

$$\frac{1}{k!}\binom{n+k+c}{k-1} = \frac{1}{k!(k-1)!} \cdot \frac{(n+k+c)!}{(n+1+c)!}.$$

Mit Hilfe der Stirlingschen Formel zeigen wir hier

$$\frac{(n+k+c)!}{(n+1+c)!} \sim n^{k-1}$$

für $k = o(n^{1/3})$. Es ergibt sich

$$\frac{(n+k+c)!}{n^{k-1}(n+1+c)!} \sim \frac{(n+k+c)^{n+k+c}}{n^{k-1}(n+1+c)^{n+1+c}} \sqrt{\frac{n+k+c}{n+1+c}}\, e^{1-k}$$

$$\sim e^{1-k+(n+k+c)\log\left(1+\frac{k+c}{n}\right)-(n+1+c)\log\left(1+\frac{1+c}{n}\right)} = e^{O(k^2/n)} \sim 1.$$

Für $k = o(n^{1/3})$ ist daher

$$\frac{1}{k!}\binom{n+k+c}{k-1} \sim \frac{n^{k-1}}{k!(k-1)!}. \tag{6}$$

Die asymptotischen Darstellungen (5) und (6) geben in Verbindung mit Satz 7.7 die Behauptung.

7.3. Die Anzahl der nicht-isomorphen abelschen Gruppen n-ter Ordnung

Wir knüpfen an die Ausführungen in 3.1 an. Dort hatten wir für die Anzahl $a(n)$ der nicht-isomorphen abelschen Gruppen bereits erkannt:

$$(m, n) = 1 \Rightarrow a(mn) = a(m)\, a(n),$$

$$n = \prod_{i=1}^{r} p_i^{\nu_i} \Rightarrow a(n) = \prod_{i=1}^{r} a(p_i^{\nu_i}) = \prod_{i=1}^{r} (P\nu_i).$$

Jetzt wollen wir eine erzeugende Funktion für $a(n)$ aufstellen. Auf Grund der trivialen Abschätzung $a(n) \leqq \frac{n}{2}$ für $n > 1$ gibt es ein s_0, so daß für alle $s > s_0$ die Reihe

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

konvergiert. Dann ist nach Satz 5.7 und nach (3)

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \prod_p \left(\sum_{\nu=0}^{\infty} \frac{a(p^\nu)}{p^{\nu s}} \right) = \prod_p \left(\sum_{\nu=0}^{\infty} \frac{P(\nu)}{p^{\nu s}} \right)$$
$$= \prod_p \prod_{n=1}^{\infty} (1 - p^{-ns})^{-1} = \prod_{n=1}^{\infty} \prod_p (1 - p^{-ns})^{-1}.$$

Damit ist sogar für $s > 1$

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \prod_{n=1}^{\infty} \zeta(ns). \tag{7}$$

Schreibt man noch die Reihendarstellung der Funktion $\zeta(ns)$ auf, so erkennt man, daß $a(n)$ mit der Anzahl der Zerlegungen von n in

$$n = n_1 n_2^2 n_3^3 \cdots, \tag{8}$$

$n_1, n_2, \ldots \in \mathbf{N}$, übereinstimmt.

Nun wollen wir uns mit den in Kapitel 6 entwickelten Größenordnungen auseinandersetzen.

Satz 7.9 (KRÄTZEL). *Die maximale Größenordnung von $\log a(n)$ ist*

$$\frac{\log 5}{4} \cdot \frac{\log n}{\log \log n}.$$

Das heißt, es ist mit $\varepsilon > 0$

$$a(n) < 5^{\frac{1+\varepsilon}{4} \cdot \frac{\log n}{\log \log n}} \tag{9}$$

für $n > N(\varepsilon)$ und

$$a(n) > 5^{\frac{1-\varepsilon}{4} \cdot \frac{\log n}{\log \log n}} \tag{10}$$

für unendlich viele n.

Beweis. Wir ziehen den Satz 5.27 heran. In den dortigen Bezeichnungen ist $f(n) = a(n), f(p^\nu) = a(p^\nu) = P(\nu)$, also $g(\nu) = P(\nu)$. Nach Satz 7.6 ist $\log P(\nu) = O(\nu^{1/2})$,

so daß in Satz 5.27a $= \frac{1}{2}$ gewählt werden kann. Nach Satz 7.5 ist

$$P(\nu) \leqq 5^{\nu/4} \quad \text{für} \quad \nu \leqq 4,$$
$$< 5^{\nu/4} \quad \text{für} \quad \nu > 4,$$

so daß mit $k = 4$, $g(4) = 5$ der Satz 5.27 sofort die Behauptung ergibt.

Wir wenden uns jetzt der durchschnittlichen Größenordnung von $a(n)$ zu. Es bezeichne

$$A(x) = \sum_{n \leqq x} a(n)$$

und

$$c_n = \prod_{\substack{\nu=1 \\ \nu \nmid n}}^{\infty} \zeta\left(\frac{\nu}{n}\right) \quad (n = 1, 2, \ldots). \tag{11}$$

P. Erdös und G. Szekeres zeigten 1934, daß $a(n)$ die durchschnittliche Größenordnung c_1 $(2{,}29 < c_1 < 2{,}3)$ hat. Genauer zeigten sie

$$A(x) = c_1 x + O\left(\sqrt{x}\right).$$

Dieses Ergebnis wurde 1947 von D. G. Kendall und R. A. Rankin zu

$$A(x) = c_1 x + c_2 x^{1/2} + O(x^{1/3} \log^2 x)$$

verbessert. Dies kann mit relativ einfachen Mitteln selbst bei Reduzierung noch eines logarithmischen Faktors erreicht werden.

Satz 7.10. *Mit* (11) *gilt*

$$A(x) = c_1 x + c_2 x^{1/2} + O(x^{1/3} \log x).$$

Beweis. Für $k \in \mathbf{N}$ bezeichne

$$a_k(n) = \sum_{n_k n_{k+1}^{k+1} \cdots = n} 1, \qquad a_1(n) = a(n), \tag{12}$$

so daß wir für $s > \frac{1}{k}$

$$\sum_{n=1}^{\infty} \frac{a_k(n)}{n^s} = \prod_{n=k}^{\infty} \zeta(ns)$$

erhalten. Dann ist mit Satz 5.40

$$A(x) = \sum_{nm \leqq x} d(1, 2; n)\, a_3(m)$$
$$= \sum_{m \leqq x} a_3(m) \left\{ \zeta(2) \frac{x}{m} + \zeta\left(\frac{1}{2}\right) \left(\frac{x}{m}\right)^{1/2} + O\left(\left(\frac{x}{m}\right)^{1/3}\right) \right\}. \tag{13}$$

Für $\nu = 1, \frac{1}{2}$ folgt

$$\sum_{m \leqq x} \frac{a_3(m)}{m^\nu} = \sum_{m=1}^{\infty} \frac{a_3(m)}{m^\nu} - \sum_{m > x} \frac{a_3(m)}{m^\nu} = \sum_{m=1}^{\infty} \frac{a_3(m)}{m^\nu} - \sum_{n^2 m > x} \frac{a_4(m)}{(n^2 m)^\nu}.$$

Die Abschätzung der Restsumme ergibt

$$\sum_{n^3m>x} \frac{a_4(m)}{(n^3m)^r} = \sum_{m\le x} \frac{a_4(m)}{m^r} \sum_{n^3>x/m} \frac{1}{n^{3r}} + \sum_{m>x} \frac{a_4(m)}{m^r} \sum_{n=1}^{\infty} \frac{1}{n^{3r}}$$

$$= O\left(\sum_{m\le x} \frac{a_4(m)}{m^r} \int_{\left[\left(\frac{x}{m}\right)^{1/3}\right]}^{\infty} \frac{1}{t^{3r}}\, dt \right) + O\left(\sum_{m>x} \frac{a_4(m)}{m^r} \right)$$

$$= O\left(x^{\frac{1}{3}-r} \sum_{m\le x} \frac{a_4(m)}{m^{1/3}} \right) + O\left(x^{\frac{1}{3}-r} \sum_{m>x} \frac{a_4(m)}{m^{1/3}} \right) = O\left(x^{\frac{1}{3}-r} \right).$$

Damit ist

$$\sum_{m\le x} \frac{a_3(m)}{m} = \frac{c_1}{\zeta(2)} + O(x^{-2/3}), \tag{14}$$

$$\sum_{m\le x} \frac{a_3(m)}{m^{1/2}} = \frac{c_2}{\zeta\left(\frac{1}{2}\right)} + O(x^{-1/6}). \tag{15}$$

Für die Abschätzung des Restes in (13) vermerken wir zunächst

$$\sum_{m\le x} a_3(m) = \sum_{n^3m\le x} a_4(m) = O\left(\sum_{m\le x} a_4(m) \left(\frac{x}{m}\right)^{1/3} \right) = O(x^{1/3})$$

und sodann vermittels der Abelschen Identität

$$\sum_{m\le x} a_3(m) \left(\frac{x}{m}\right)^{1/3} = \sum_{m\le x} a_3(m) + \frac{1}{3} \int_1^x \left(\frac{x}{t}\right)^{1/3} \sum_{m\le t} a_3(m) \frac{dt}{t} = O(x^{1/3} \log x). \tag{16}$$

Trägt man (14), (15), (16) in (13) ein, so erhält man die Behauptung.

Im Jahre 1952 konnte H. E. Richert erstmals die Größenordnung $x^{1/3}$ im Fehlerglied unterbieten und zeigte

$$A(x) = c_1 x + c_2 x^{1/2} + c_3 x^{1/3} + \Delta(x)$$

mit

$$\Delta(x) = O((x^3 \log^9 x)^{1/10}).$$

Im Verlaufe der folgenden Jahre wurde diese Abschätzung von verschiedenen Autoren weiter verbessert. Das beste Resultat hält gegenwärtig B. R. Srinivasan, er erzielte 1973

$$\Delta(x) = O(x^{105/407} \log^2 x).$$

Mit Hilfe der in 6.5.2. entwickelten Vinogradovschen Methode erzielte P. G. Schmidt 1968 das Ergebnis

$$\Delta(x) = O((x^2 \log^4 x)^{1/7}).$$

Im Sinne der Definition 5.20 kann $a(n)$ keine normale Größenordnung besitzen. Denn für quadratfreies n ist $a(n) = 1$, und nach Satz 5.41 ist

$$\sum_{\substack{a(n)=1 \\ n\le x}} 1 = \sum_{n\le x} |\mu(n)| = \frac{6}{\pi^2} x + O(\sqrt{x}). \tag{17}$$

Interessant ist nun aber, daß eine Verteilung der Werte n mit $a(n) = m$ für beliebiges $m \geqq 0$ überschaubar dargestellt werden kann. Es wird sich allgemein die asymptotische Darstellung

$$\sum_{\substack{a(n)=m \\ n \leq x}} 1 \sim P_m x$$

ergeben.

Für den Nachweis dieser Darstellung betrachten wir zunächst die für $s > 1$ konvergenten Dirichletschen Reihen

$$A_m(s) = \sum_{\substack{n=1 \\ a(n)=m}}^{\infty} \frac{1}{n^s}$$

mit $m = 0, 1, 2, \ldots$ Da $a(n)$ stets positiv ist, haben wir $A_0(s) \equiv 0$. Wie schon bekannt, ist

$$A_1(s) = \sum_{n=1}^{\infty} \frac{|\mu(n)|}{n^s} = \frac{\zeta(s)}{\zeta(2s)}. \tag{18}$$

Um für $m > 1$ zu einer Darstellung von $A_m(s)$ zu gelangen, zerlegen wir die Zahlen n in $n = n_1 n_2$ mit $(n_1, n_2) = 1$, wobei außerdem n_1 eine *Zahl zweiter Art* und n_2 *quadratfrei* sein sollen. Dabei wird eine Zahl von zweiter Art genannt, wenn jeder Primfaktor mindestens in zweiter Potenz enthalten ist. Dann ist $a(n) = a(n_1)$, und wir erhalten

$$A_m(s) = \sum_{a(n_1)=m} \frac{1}{{n_1}^s} \sum_{(n_1,n_2)=1} \frac{1}{{n_2}^s},$$

wobei in der inneren Summe über alle quadratfreien Zahlen n_2 und in der äußeren Summe über alle Zahlen zweiter Art n_1 zu summieren ist. Für die innere Summe haben wir

$$\sum_{(n_1,n_2)=1} \frac{1}{{n_2}^s} = \sum_{\substack{k=1 \\ (n_1,k)=1}}^{\infty} \frac{|\mu(k)|}{k^s} = \sum_{k=1}^{\infty} \frac{f(k)}{k^s}$$

mit

$$f(k) = \begin{cases} |\mu(k)| & \text{für} \quad (n_1, k) = 1, \\ 0 & \text{für} \quad (n_1, k) > 1. \end{cases}$$

Wegen der Multiplikativität von $f(k)$ erhalten wir in Anwendung von Satz 5.7

$$\sum_{(n_1,n_2)=1} \frac{1}{{n_2}^s} = \prod_p \left(\sum_{\nu=0}^{\infty} \frac{f(p^\nu)}{p^{\nu s}} \right) = \prod_{p \nmid n_1} \left(\sum_{\nu=0}^{\infty} \frac{|\mu(p^\nu)|}{p^{\nu s}} \right)$$

$$= \prod_{p \nmid n_1} \left(1 + \frac{1}{p^s} \right) = \frac{\zeta(s)}{\zeta(2s)} \prod_{p \mid n_1} \left(1 + \frac{1}{p^s} \right)^{-1}.$$

Insgesamt ergibt sich hieraus

$$A_m(s) = \frac{\zeta(s)}{\zeta(2s)} B_m(s) \tag{19}$$

mit $B_1(s) = 1$ wegen (18) und

$$B_m(s) = \sum_{a(n_1)=m} \frac{1}{n_1^{\,s}} \sum_{p \mid n_1} \left(1 + \frac{1}{p^s}\right)^{-1} \tag{20}$$

für $m \geqq 2$. Bei der für $s > \frac{1}{2}$ konvergenten Reihe ist wieder über alle Zahlen zweiter Art n_1 zu summieren. Speziell ist

$$B_2(s) = \sum_p \frac{1}{p^s(p^s + 1)},$$

wobei die Summe über alle Primzahlen zu führen ist. Damit sind die notwendigen Vorbereitungen getroffen.

Satz 7.11 (Kendall/Rankin). *Für $m = 0, 1, 2, \ldots$ existieren die Grenzwerte*

$$\lim_{x \to \infty} \frac{1}{x} \sum_{\substack{n \leqq x \\ a(n)=m}} 1 = P_m.$$

Dabei sind die P_m durch

$$P_0 = 0, \qquad P_1 = \frac{6}{\pi^2}, \qquad P_m = \frac{6}{\pi^2} B_m(1) \qquad (m \geqq 2) \tag{21}$$

mit $B_m(1)$ aus (20) gegeben. Und es gilt

$$\sum_{m=0}^{\infty} P_m = 1, \tag{22}$$

$$\sum_{m=0}^{\infty} m P_m = c_1 = \lim_{x \to \infty} \frac{1}{x} \sum_{n \leqq x} a(n). \tag{23}$$

Beweis. (21) ist für $m = 0$ trivial und folgt für $m = 1$ aus (17). Für $m \geqq 2$ setzen wir

$$B_m(s) = \sum_{n=1}^{\infty} \frac{b_m(n)}{n^s},$$

wobei die Konvergenz der Reihe für $s > \frac{1}{2}$ gesichert ist. Nach (19) und (17) ist

$$\begin{aligned} \frac{1}{x} \sum_{\substack{n \leqq x \\ a(n)=m}} 1 &= \frac{1}{x} \sum_{n_1 n_2 \leqq x} |\mu(n_1)|\, b_m(n_2) \\ &= \frac{6}{\pi^2} \sum_{n \leqq x} \left\{ \frac{b_m(n)}{n} + O\left(x^{\vartheta - 1} \frac{b_m(n)}{n^\vartheta}\right) \right\} \end{aligned}$$

mit $\frac{1}{2} < \vartheta < 1$. Für $x \to \infty$ folgt hieraus sofort (21).

Die unendlichen Reihen in (22) und (23) sind konvergent, denn die Folgen ihrer Partialsummen

$$S_M = \sum_{m=0}^{M} P_m, \qquad T_M = \sum_{m=0}^{M} mP_m$$

sind monoton wachsend und wegen

$$S_M \leqq T_M = \lim_{x\to\infty} \frac{1}{x} \sum_{m=1}^{M} m \sum_{\substack{n\leqq x \\ a(n)=m}} 1 \leqq \lim_{x\to\infty} \frac{1}{x} \sum_{n\leqq x} a(n) = c_1$$

nach oben beschränkt. Dann erhalten wir bei Berücksichtigung von (20), (21) und des Satzes 5.7

$$\begin{aligned}\sum_{m=0}^{\infty} P_m &= \frac{1}{\zeta(2)} \sum_{m=1}^{\infty} \sum_{\substack{n_1=1 \\ a(n_1)=m}}^{\infty} \frac{1}{n_1} \prod_{p\mid n_1} \left(1+\frac{1}{p}\right)^{-1} = \frac{1}{\zeta(2)} \sum_{n_1=1}^{\infty} \frac{1}{n_1} \prod_{p\mid n_1} \left(1+\frac{1}{p}\right)^{-1} \\ &= \frac{1}{\zeta(2)} \prod_p \left(1+\frac{p}{p+1} \sum_{\nu=2}^{\infty} \frac{1}{p^\nu}\right) = \frac{1}{\zeta(2)} \prod_p \left(\frac{p}{p+1} \sum_{\nu=0}^{\infty} \frac{1}{p^\nu}\right) \\ &= \frac{1}{\zeta(2)} \prod_p \left(1-\frac{1}{p^2}\right)^{-1} = 1.\end{aligned}$$

Das ist (22). Ebenso erfolgt der Nachweis von (23), nur benötigen wir hier zusätzlich (3).

$$\begin{aligned}\sum_{m=0}^{\infty} mP_m &= \frac{1}{\zeta(2)} \sum_{m=1}^{\infty} m \sum_{\substack{n_1=1 \\ a(n_1)=m}}^{\infty} \frac{1}{n_1} \prod_{p\mid n_1} \left(1+\frac{1}{p}\right)^{-1} \\ &= \frac{1}{\zeta(2)} \sum_{n_1=1}^{\infty} \frac{a(n_1)}{n_1} \prod_{p\mid n_1} \left(1+\frac{1}{p}\right)^{-1} \\ &= \frac{1}{\zeta(2)} \prod_p \left(1+\frac{p}{p+1} \sum_{\nu=2}^{\infty} \frac{a(p^\nu)}{p^\nu}\right) = \frac{1}{\zeta(2)} \prod_p \left(\frac{p}{p+1} \sum_{\nu=0}^{\infty} \frac{P(\nu)}{p^\nu}\right) \\ &= \frac{1}{\zeta(2)} \prod_p \left\{\left(1+\frac{1}{p}\right)^{-1} \prod_{k=1}^{\infty} \left(1-\frac{1}{p^k}\right)^{-1}\right\} = \prod_{\nu=2}^{\infty} \zeta(\nu) = c_1.\end{aligned}$$

7.4. Aufgaben

Bei den folgenden Aufgaben bedeute mit $k \in \mathbf{N}$ die zahlentheoretische Funktion $P_\nu(n; k)$ die Anzahl der Darstellungen von n in der Form

$$n = m_1 + 2^k m_2 + 3^k m_3 + \cdots + \nu^k m_\nu$$

mit ganzen Zahlen $m_1, m_2, \ldots, m_\nu \geqq 0$. Weiter sei

$$P(n; k) := \lim_{\nu\to\infty} P_\nu(n; k).$$

1. Man beweise für $|z| < 1$

$$\sum_{n=0}^{\infty} P_\nu(n; k) = \prod_{m=1}^{\nu} (1 - z^{m^k})^{-1},$$

$$\sum_{n=0}^{\infty} P(n; k) = \prod_{m=1}^{\infty} (1 - z^{m^k})^{-1}.$$

2. Mit der Vereinbarung $P_\nu(n; k) = 0$ für $n < 0$ weise man die Differenzengleichung

$$P_\nu(n; k) = P_\nu(n - \nu^k; k) + P_{\nu-1}(n, k)$$

für $\nu \geqq 2$ nach.

3. $P_2(n; k) = \left[\frac{n}{2^k}\right] + 1.$

4. $\frac{1}{2 \cdot 6^k} n^2 - \frac{1}{2^{k+1}} n < P_3(n; k) < \frac{1}{2 \cdot 6^k} n^2 + \left(\frac{3}{2^{k+1}} + \frac{1}{3^k}\right) n + 1.$

5. Man beweise

$$P(n; k) < a_k n^{-\frac{k}{k+1}} e^{b_k n^{\frac{1}{k+1}}}$$

Dabei ist mit der Gammafunktion $\Gamma(z)$

$$a_k = \left(\frac{1}{k^2} \Gamma\left(\frac{1}{k}\right) \zeta\left(1 + \frac{1}{k}\right)\right)^{\frac{k}{k+1}}, \qquad b_k = (k + 1)\, a_k.$$

6. Es ist für $\varepsilon > 0$ die Ungleichung

$$a(n) < (\log n)^{\frac{1}{4}\log 5 + \varepsilon}$$

für fast alle n nachzuweisen. — E. Krätzel.

Literatur

[1] Apostol, T. M., Introduction to Analytic Number Theory, Springer-Verlag, New York—Heidelberg—Berlin 1976.

[2] Asser, G., Grundbegriffe der Mathematik. I. Mengen. Abbildungen. Natürliche Zahlen, 4. überarb. und erg. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1980.

[3] Khintchine, A. J., Kettenbrüche, B. G. Teubner Verlagsgesellschaft, Leipzig 1956.

[4] Enzyklopädie der Elementarmathematik, Bd I. 8. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1978.

[5] Flachsmeyer, J., und L. Prohaska, Algebra. 4. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1980.

[6] Gelfond, A. O., and Yu. V. Linnik, Elementary Methods in Analytic Number Theory. Rand Mc. Nally & Company, Chicago 1965.

[7] Hardy, G. H., and E. M. Wright, An Introduction to the Theory of Numbers, At the Clarendon Press Oxford 1960.

[8] Hasse, H., Vorlesungen über Zahlentheorie. Springer-Verlag, Berlin—Göttingen—Heidelberg 1950.

[9] Koch, H., und H. Pieper, Zahlentheorie. Ausgewählte Methoden und Ergebnisse. VEB Deutscher Verlag der Wissenschaften, Berlin 1976.

[10] Landau, E., Handbuch der Lehre von der Verteilung der Primzahlen I, II. B. G. Teubner, Leipzig und Berlin 1909.

[11] Landau, E., Vorlesungen über Zahlentheorie, I. Aus der elementaren und additiven Zahlentheorie. S. Hirzel, Leipzig 1927.

[12] Mitrinović, D. S., and M. S. Popadić, Inequalities in Number Theory, Niš 1978.

[13] Nagell, T., Introduction to Number Theory. Almqvist & Wiksell, Stockholm 1951.

[14] Perron, O., Die Lehre von den Kettenbrüchen I. Elementare Kettenbrüche. B. G. Teubner Verlagsgesellschaft, Stuttgart 1954.

[15] Perron, O., Irrationalzahlen. de Gruyter, Berlin 1910.

[16] Prachar, K., Primzahlverteilung. Springer-Verlag, Berlin—Göttingen—Heidelberg 1957.

[17] Schwarz, W., Einführung in Methoden und Ergebnisse der Primzahltheorie. Bibliographisches Institut, Mannheim/Wien/Zürich 1969.

[18] Sierpiński, W., Elementary Theory of Numbers. PWN, Warszawa 1964.

[19] Winogradow, I. M., Elemente der Zahlentheorie. VEB Deutscher Verlag der Wissenschaften, Berlin 1955.

Weiterhin sei auf das Bändchen

Drinfel'd, G. I., Quadratur des Kreises und Transzendenz von π, VEB Deutscher Verlag der Wissenschaften, Berlin 1980 (Übersetzung aus dem Russischen)

hingewiesen.

Namen- und Sachverzeichnis

abelsche Gruppen, Anzahl 209
— —, endliche 45
— Identität 97
Abschätzung der n-ten Primzahl 11, 103
— der Anzahl der Partitionen 205, 206, 207
Abschnitt eines Kettenbruches 66
Abzählbarkeit der algebraischen Zahlen 77
algebraische Zahl 77
— —, Abzählbarkeit 77
Algorithmus, Euklidischer 14
Anzahl abelscher Gruppen endlicher Ordnung 209
— der Darstellungen natürlicher Zahlen als Summe von Quadraten 165
— der Partitionen einer Zahl 46, 201
— der Primfaktoren einer natürlichen Zahl 47
— der Primzahlen 103
— der quadratfreien Zahlen 136
Approximation, beste 74
— zur Ordnung n 76
— reeller Zahlen durch rationale Zahlen 73
Äquivalenzrelation 17
Archimedes 76
arithmetische Progression 102
asymptotisch gleiche Funktion 97

Bachet, C. G. 163, 178
beste Approximation 74
biquadratischer Rest 44

Cantor, G. 79
—, Satz von 79
Charakter 48
Charaktergruppe 49
Čebyšev, P. L. 87, 106, 108, 111
—, Satz von 108
Čebyševsche Ergebnisse 108, 110
— Funktion $\vartheta(x)$ 106
— — $\psi(x)$ 106
Corput, J. G. van der 192, 195

Darstellung von natürlichen Zahlen als Quadratsummen 133, 162
— von Primzahlen als Quadratsummen 152
Diophant 24, 178
diophantische Gleichungen, lineare 24
— — dritten Grades 177
— — vierten Grades 178
— — zweiten Grades 172, 174
direktes Produkt 45
Dirichlet, P. G. L. 87, 135, 195
—, Satz von 135
Dirichletsche Multiplikation 88
— Reihe 92
—s Produkt 87
Division im Restklassenring 18
— mit Rest 14
Duncan, R. L. 138
—, Satz von 138
durchschnittliche Größenordnung 132

Einheitswurzel 48
endliche Gruppe, abelsche 45
— —, — Hauptsatz 45
Eratosthenes 105
Erdös, P. 112, 192, 207, 208, 211
Ergänzungssätze zum quadratischen Reziprozitätsgesetz 42
Ergebnisse, Čebyševsche 108, 110
Euklid 10
Euklidischer Algorithmus 14
Euler, L. 20, 22, 36, 95, 104, 163
Eulersche φ-Funktion 20, 91, 96, 127, 130, 132
— Identität 164
— Konstante 100, 109
—s Kriterium 38
Euler-Maclaurinsche Summenformel 98
Exponentialkongruenz 32

Fermat, P. de 22, 178
Fermatscher Satz, großer 178
— —, kleiner 22
Fermat-Euler, Satz von 22

Formel, Selbergsche 113
—, Stirlingsche 101
Formeln, Möbiussche 91
Fourier, J. B. J. 80
Fuchs, W. H. J. 192
Fundamentallösung 155
— der Klasse K 160
Fundamentalsatz der Zahlentheorie 11
φ-Funktion, Eulersche 20, 91, 96, 127, 130
Funktion, Jordansche 131
—, Liouvillesche 146
—, Mangoldtsche 91, 96
μ- —, Möbiussche 90, 95, 140
—, multiplikative zahlentheoretische 89
—, total multiplikative zahlentheoretische 89
—, zahlentheoretische 87
Funktionen, asymptotisch gleiche 97
—, Čebyševsche $\vartheta(x)$, $\psi(x)$

Gauss, C. F. 17, 36, 37, 40, 42, 55, 61, 111, 133, 167, 179, 191
—, Satz von 42, 61, 133, 167
Gaußsche Summe 52
— —, quadratische 55
—s Lemma 40
Gitterpunkte 24, 149
— auf einem Kreis 153, 181, 190
— auf Ellipsen 151
— auf Hyperbeln 154, 194
— auf Parabeln 150
— in mehrdimensionalen Kugeln 197
— unterhalb einer Hyperbel 194
Gleichung, lineare diophantische 24
—, pythagoräische 173
—en, diophantische dritten Grades 177
—en, diophantische vierten Grades 178
—en, diophantische zweiten Grades 178
Gronwall, T. H. 122
—, Satz von 122
Größenordnung zahlentheoretischer Funktionen, durchschnittliche 132
— — —, maximale 122
— — —, normale 145
größter gemeinsamer Teiler 13
Gruppe, endliche abelsche 45
—, zyklische 45
Gupta, H. 207
—, Satz von 207

Hadamard, J. 112
Hardy, G. H. 136, 145, 191, 195, 207
Hauptcharakter 48
Hauptsatz für endliche abelsche Gruppen 45
Hermite, C. 81
—, Satz von 82

Identität, Abelsche 97
—, Eulersche 164
Index 31
Indexrechnung 31
Indextafel 32
Inkongruenz 17
Integraldarstellung der Riemannschen Zetafunktion 100
irrationale Zahl 71
Irrationalität, quadratische 71
— von e 80
— von π 80

Jacobi, C. G. J. 167, 169
—, Satz von 169
Jordansche Funktion 131

kanonische Zerlegung 12
Kendall, D. G. 211, 214
Kettenbruch 66
—, Abschnitt 66
— mit natürlichen Elementen 68
—, periodischer 71
kleiner Fermatscher Satz 22
kleinstes gemeinsames Vielfaches 14
Kolesnik, G. A. 195
Kongruenz 17
—, lineare 17, 22
—, quadratische 36
—en, simultane lineare 25
Kongruenzrelation 17
Konstante, Eulersche 100
Krätzel, E. 123, 147, 148, 193, 200, 205, 210, 216
—, Satz von 123, 205, 210
Kreisproblem 191
Kriterium, Eulersches 38

Lagrange, J. L. 74, 163
—, Satz von 74, 163
Lambert, J. H. 80
—, Sätze von 80
Landau, E. 97, 128, 167, 192
—, Satz von 128
Landau-Symbole
Langford, E. S. 147
Lauffer 16
Legendre, A. M. 36, 37, 111, 174
—, Satz von 174
Legendre-Symbol 38, 42, 51
— —, transzendente Darstellung

Lehner, J. 208
Lemma, Gaußsches 40
Lindemann, F. 81
—, Satz von 83
Lindner, C. C. 147
lineare diophantische Gleichung 24
— Kongruenz 17, 23
— Kongruenz, simultane 25
Liouville, J. 78
—, Satz von 78
Liouvillesche Funktion $\lambda(n)$ 146

Makowski, A. 147
Mangoldtsche Funktion 91, 96
maximale Größenordnung 122
Mertens, F. 132
—, Satz von 132
Methode des unbegrenzten Abstiegs 177
Methode, Vinogradovsche 182, 194
Metius, A. 76
Möbius, A. F. 90
Möbiussche Formeln 91
— μ-Funktion 90, 95, 140
Modul 17
multiplikative zahlentheoretische Funktion 89

Näherungsbruch 67
Newman, D. 207
Niven, J. 80
normale Größenordnung 145
Nullteiler im Restklassenring 19

Partition 46, 201
—, Anzahl 46, 201
periodischer Kettenbruch 71
Pòlya, G. 15
Polynomkongruenz 33
Porubski, S. 147
Potenzrest 33
prime Restklasse 20
— Restklassengruppe 20, 27
Primfaktoren, Anzahl 47
primitive Wurzel 27
—r Restklassencharakter 53
Primteiler 10
Primzahl 10, 152
—, Abschätzung 10
—, Anzahl 103
—en in arithmetischen Progressionen 102
Primzahlfunktion 101
Primzahlkriterium 23
Primzahlsatz 116, 140
primzahlunabhängige Funktion 125
Produkt, direktes 45
Produkt, Dirichletsches 87
Produktdarstellung der quadratischen Gaußschen Summe 57
Punkte, rationale auf dem Einheitskreis 172
—, — auf einer Kurve 170
—, — auf Ellipsen 171
—, — auf Hyperbeln 171
—, — auf Parabeln 170
Pythagoräische Gleichung 173
— Zahlentripel 173

quadratfrei 136
—e Zahlen 95, 136
quadratische Gaußsche Summe 55
— — —, Produktdarstellung 57
— Irrationalität 71
— Kongruenz 36
—r Rest 36
—r Restklassencharakter 51, 52
—s Reziprozitätsgesetz 36
—s —, Ergänzungssätze 42

Rademacher, H. 207
Ramanujan, S. 129, 136, 145, 207
Ramanujansche Reihe 129
— Summe 52, 129
Randol, B. 192
Rankin, R. A. 211, 214
rationale Punkte auf dem Einheitskreis 172
— — auf einer Kurve 170
— — auf Ellipsen 173
— — auf Hyperbeln 173
— — auf Parabeln 170
reelle Zahlen, Approximation 73
— —, Überabzählbarkeit 79
Reihe, Dirichletsche 92
—, Ramanujansche 129
Rest, biquadratischer 44
—, quadratischer 36
Restgleichheit 17
Restklasse 17
—, prime 20
Restklassencharakter 50
—, primitiver 53
—, quadratischer 51, 54
Restklassengruppe, prime 20, 27
Restklassenring 18
Restsystem, vollständiges 18
Reziprozitätsgesetz, quadratisches 36, 42, 55
— für die quadratischen Gaußschen Summen 55
Richert, H. E. 195, 212
Riemann, B. 95
Riemannsche Zetafunktion 95
— —, Integraldarstellung 100

Satyanarayana, M. 147
Satz, großer Fermatscher 178
—, kleiner Fermatscher 22
— von Cantor 79
— von Čebyšev 108
— von Dirichlet 135
— von Duncan 138
— von Erdös/Lehner 208
— von Fermat-Euler 22
— von Gauss 42, 61, 133, 167
— von Gronwall 122
— von Gupta 207
— von Hardy-Ramanujan 136, 145
— von Jacobi 169
— von Kendall/Rankin 214
— von Krätzel 123, 205, 210
— von Lagrange 74, 163
— von Landau 128
— von Legendre 174
— von Liouville 78
— von Mertens 132
— von Turán 138
— von Vinogradov 178, 184
— von Wigert 127
— von Wilson 23
Sätze von Lambert 80
Schmidt, P. G. 212
Selberg, A. 112
Selbergsche Formel 113
— Ungleichung 116
Sieb von Eratosthenes 105
Sierpiński, W. 16, 147, 191, 200
simultane lineare Kongruenz 25
Sivaramakrishnan, R. 147
Srinivasan, B. R. 212
Steinhaus, H. 200
Stirlingsche Formel 101
Summe, Gaußsche 52
—, quadratische Gaußsche 55
—, Ramanujansche 52, 129
Summenformel, Euler-Maclaurinsche 98
Surányi, J. 11
Szekeres, G. 208, 211

Teilbarkeit 9
Teiler, größter gemeinsamer 13
Teilerfremdheit 13, 25
Teilerfunktion 89, 95, 121
Teilerproblem 195
Teufel, E. 148
total multiplikative zahlentheoretische Funktion 89
transzendente Zahl 78
Transzendenz von e 81
— von π 81
Turan, P. 137, 138
—, Satz von 138

Überabzählbarkeit der reellen Zahlen 79
Ungleichung, Selbergsche 116

Vallée-Poussin, C. de la 112
Venkataraman, C. S. 147
Vielfaches, kleinstes gemeinsames 14
Vinogradov, I. M. 149, 179, 182, 184, 191, 195
—, Satz von 184
Vinogradovsche Methode 182, 194
vollständiges Restsystem 18
Voronoi, G. F. 191

Weil, K. 161
Wigert, S. 127
—, Satz von 127
Wilson, Satz von 23
Wright, E. M. 112
Wurzel, primitive 27

Yin, Wen-lin 192

Zahl, algebraische 77
—, irrationale 71
—, quadratfreie 95, 136
—, transzendente 78
—, zusammengesetzte 10
—en zweiter Art 77
zahlentheoretische Funktion 87
— —, multiplikative 89
— —, totale multiplikative 89
zahlentheoretische Funktion $\varphi(n)$ 20, 91, 96, 127
— — $P(n)$ 46
— — $a(n)$ 46, 210
— — $\omega(n)$ 47, 136, 145
— — $\Omega(n)$ 47, 136, 145
— — $\sigma_k(n)$ 134
— — $d(n)$ 135, 145
— — $\mu(n)$ 90, 95, 140
— — $\Lambda(n)$ 91, 96, 140
— — $J_k(n)$ 131
— — $r(n)$ 133
— — $r_k(n)$ 165, 181
— — $\lambda(n)$ 146
— — $\lambda_k(n)$ 146
— — $q_k(n)$
— — $d(a, b; n)$
Zahlentripel, Pythagoräische 173
zusammengesetzte natürliche Zahl 143
— Zahl 10
Zerlegung, kanonische 12
zyklische Gruppe 45