L. G. Lucht

Elementare Zahlentheorie

Technische Universität Clausthal
Institut für Mathematik

SS 1998

Als Manuskript vervielfältigt

In dieser Ausarbeitung ist eine Auswahl von Problemen, Methoden und Resultaten aus Vorlesungen über elementare Zahlentheorie dargestellt, die ich einige Male an der Technischen Universität Clausthal gehalten habe. Im Sommersemester 1994 hatte ich die Vorlesung wie folgt eingeleitet:

„In manchen Kreisen gilt es als schick, von Mathematik möglichst wenig zu verstehen. Ein sehr hilfreiches Argument besteht darin zu sagen, daß Mathematik in der Praxis ziemlich unnütz sei. In manchen Mathematikerkreisen gilt es als schick, von Zahlentheorie möglichst wenig zu verstehen. Ein sehr hilfreiches Argument besteht darin zu sagen, daß Zahlentheorie in der Praxis ziemlich unnütz sei. Ich biete meine Vorlesung für alle diejenigen an, denen mehr an Erkenntnissen als am Schicksein liegt."

Für die Überlassung der LaTeX Version seiner Mitschrift der Vorlesung und vielfältige Unterstützung bei der Umsetzung des Manuskripts sowie für das Korrekturlesen bin ich Herrn Dipl.-Math. Martin Traupe zu besonderem Dank verpflichtet.

Inhaltsverzeichnis

Kapitel 1

Probleme der Zahlentheorie

Dieser Kapitel beschreibt einige Probleme der Zahlentheorie, ihre Herkunft und ihre Entwicklung.

1.1 Beispiele im Dutzend

Arithmetische und geometrische Probleme sind zum Teil sehr alt. Sie entstanden in den babylonischen und griechischen Hochkulturen aus praktischen Bedürfnissen wie etwa Landvermessung, Zeiteinteilung, Handel, Religion. Die Mathematik des Altertums (ca. 2000 v. Chr. bis 1000 n. Chr.) hat sie zumeist offen hinterlassen. Immerhin wurde die wissenschaftliche Vorgehensweise, bestehend aus Beobachtung, Untersuchung, Formulierung von Gesetzmäßigkeiten, Zurückführung auf Bekanntes (Beweis), im Altertum entwickelt. Die Mathematik des Mittelalters (ca. 1000 bis 1600) ist im wesentlichen durch Stagnation gekennzeichnet. Mit der Entwicklung der Infinitesimalrechnung beginnt ab ca. 1600 die Mathematik der Neuzeit.

Beispiel 1. Man beobachtet $3^2 + 4^2 = 5^2$, $5^2 + 12^2 = 13^2$, $7^2 + 24^2 = 25^2$, $8^2 + 15^2 = 17^2, \ldots$ Die geometrische Deutung, die in den Lehrsatz des Pythagoras (ca. 580 - 500 v. Chr.) einmündet, ist schon viel früher bekannt. So finden sich auf babylonischen Keilschrifttafeln (ca. 1800 v. Chr.) bereits die ersten 15 pythagoräischen Tripel $x, y, z \in \mathbb{N}$ mit $x^2+y^2 = z^2$. Die formelmäßige Bestimmung aller dieser Tripel war jedenfalls Euklid (ca. 300 v. Chr.) bekannt: (x, y, z) ist pythagoräisches Tripel von natürlichen Zahlen x, y, z genau für

$$x = 2dmn\,, \quad y = d(m^2 - n^2)\,, \quad z = d(m^2 + n^2) \qquad (d, m, n \in \mathbb{N},\ m > n)$$

bis auf Vertauschung von x, y.

Beispiel 2. In den Bereich der Zahlenmystik gehören die vollkommenen Zahlen. Dabei heißt die natürliche Zahl n vollkommen, wenn n gleich der Summe aller echten natürlichen Teiler von n ist. Man verifiziert leicht, daß etwa $6, 28, 496, 8128$ vollkommen sind; die nächste vollkommene Zahl ist 33 550 336. Die Bestimmung aller vollkommenen Zahlen ist das älteste Problem

der Mathematik. In den Bücher Euklids steht mit Beweis: Wenn $p = 2^{k+1} - 1$ Primzahl ist, so ist $n = 2^k p$ vollkommen. Euler (1707 - 1783) zeigte: Ist n gerade und vollkommen, so gilt $n = 2^k(2^{k+1} - 1)$ mit einer Primzahl $p = 2^{k+1} - 1$. Man weiß bis heute nicht, ob es endlich oder unendlich viele Primzahlen der Gestalt $2^m - 1$ gibt. (sogenannte Mersennesche Primzahlen). Leicht zu sehen ist aber, daß $2^m - 1$ nur prim sein kann, wenn der Exponent m Primzahl ist. Ungerade vollkommene Zahlen sind unbekannt, ihre Nichtexistenz ist aber unbewiesen. Die nach Mersenne (1588 - 1648) benannten Primzahlen der Form $2^m - 1$ halten regelmäßig den Weltrekord der größten bekannten Primzahlen. Die derzeit größte ist $2^{3\,021\,377} - 1$, ein Zahl mit 909 526 Dezimalstellen, die 1998 von Clarkson, Woltman, Kurowski et. al. gefunden wurde.
Eine ähnlich mystische Herkunft haben die befreundeten Zahlen. Dabei heißen natürliche Zahlen m, n befreundet, wenn die Summe der echten natürlichen Teiler von m gleich n und die Summe der echten natürlichen Teiler von n gleich m ist. Vollkommene Zahlen sind stets mit sich selbst befreundet. Das kleinste Paar verschiedener befreundeter Zahlen ist $220, 284$. Die Bibel berichtet (Genesis XXXII, 14) daß Jakob dem Esau zum Zeichen der Versöhnung 220 Schafe und 220 Ziegen schenkte. Von der Erwiderung des Freundschaftsgeschenks ist leider nichts überliefert. Ein Analogon zu Euklids Regel stellt die Regel des Thabit (1256 - 1321) dar: Sind die drei Zahlen $p = 3 \cdot 2^{k-1} - 1$, $q = 3 \cdot 2^k - 1$ und $r = 9 \cdot 2^{2k-1} - 1$ für ein $k \in \mathbb{N}$ mit $k > 1$ prim, so sind $m = 2^k pq$ und $n = 2^k r$ befreundet.

Beispiel 3. Drei bekannte, ursprünglich geometrische Probleme der Antike betreffen

a) die Trisektion (Winkeldreiteilung),

b) das Delisches Problem (Würfelverdopplung),

c) die Kreisquadratur (Überführung in ein flächengleiches Quadrat),

und zwar mittels Zirkel und Lineal als Konstruktionswerkzeug.
Alle drei Probleme konnten im Altertum nicht gelöst werden. Erst in der mathematischen Neuzeit stellte sich deren prinzipielle Unmöglichkeit aufgrund der algebraischen Merkmale von Zirkel- und Linealkonstruktionen im Zuge der Entwicklung der Algebra und der Theorie der transzendenten Zahlen heraus. Die algebraische Übersetzung lautet nämlich: Zu konstruieren sind die reellen Nullstellen der Polynome $4z^3 - 3z - \cos\alpha$ (α gegebener Winkel) und $z^3 - 2$, bzw. es ist ein Polynom mit ganzen Koeffizienten und der Nullstelle π zu finden. Insbesondere wurde letzteres 1882 von Lindemann (1852 - 1939) durch den Beweis der Transzendenz von π negativ entschieden. Zum Delischen Problem ist überliefert, daß sich die Delier an Apollo mit der Bitte um Hilfe vor einer Seuche wandten. Der Gott verlangte die Verdopplung eines ihm geweihten würfelförmigen Altars. Der Würfel mit doppelter Kantenlänge brachte keinen Erfolg, und mit der Konstruktion eines Würfels von doppeltem Volumen kamen die Delier nicht zurecht. Auch die Platonische Akademie, die um die Lösung des Problems gebeten wurde, scheiterte.
Noch heute gibt es Unbelehrbare, die sogenannten Trisektierer, Würfelverdoppler und Kreisquadrierer.

Beispiel 4. Das Altertum hat auch die Frage der Konstruierbarkeit regelmäßiger n-Ecke mit Zirkel und Lineal offen hinterlassen. Gauss (1777 - 1855) hat 1796 folgendes gezeigt: Das regelmäßige n-Eck ist genau für $n = 2^k p_1 \cdots p_r$ mit $k \in \mathbb{N}$ und $r \in \mathbb{N}_0$ konstruierbar, wobei die p_ϱ paarweise verschiedene Primzahlen der Gestalt $2^{2^\lambda} + 1$ mit $\lambda \in \mathbb{N}_0$ sind. Nach Fermat

(1601 - 1665) heißen diese Fermatsche Primzahlen. Man kennt bis heute nur fünf, nämlich $F(0) = 3$, $F(1) = 5$, $F(2) = 17$, $F(3) = 257$, $F(4) = 65\,537$. Die Vermutung von Fermat, daß alle $F(\lambda) = 2^{2^\lambda} + 1$ prim seien, hat Euler widerlegt: $641 \mid F(5) = 4\,294\,967\,297$. Leicht zu sehen ist übrigens, daß $2^k + 1$ mit $k \in \mathbb{N}_0$ nur für Zweierpotenzen k prim sein kann. Als Kuriosität wird in der Göttinger Bibliothek ein Koffer mit der expliziten (algebraischen) Konstruktion des 65 537-Ecks aufbewahrt; die Arbeit ist im Format DIN A1 abgefaßt.

Beispiel 5. Die große Fermatsche Vermutung lautet: Für kein natürliches $n \geq 3$ ist die Gleichung $x^n + y^n = z^n$ in ganzen Zahlen x, y, z mit $xyz \neq 0$ lösbar. Fermat hinterließ in einem Buch zwar die Notiz, dafür einen Beweis gefunden zu haben, für den jedoch der Rand des Buches nicht ausreiche. Erst 1995 gelang A. Wiles und R. Taylor ein Beweis der sogenannten Taniyama-Shimura-Vermutung über elliptische Kurven, aus der die Fermatsche Vermutung nach K. Ribet (1986) folgt.

Beispiel 6. Welche natürlichen Zahlen sind als Summe von höchstens m Quadratzahlen darstellbar? Die Antworten lauten für

$m = 1$: trivialerweise die Quadratzahlen selbst,
$m = 2$: die Zahlen $n = k^2 q$, wobei q keinen Primfaktor enthält, der bei Division durch 4 den Rest 3 läßt (Fermat),
$m = 3$: die Zahlen $n \neq 4^\lambda(8q + 7)$ mit $\lambda, q \in \mathbb{N}_0$ (Legendre, 1752 - 1833),
$m = 4$: alle $n \in \mathbb{N}$ (Lagrange, 1736 - 1813).

Beispiel 7. Das Waringsche Problem (1770) lautet: Trifft es zu, daß zu jedem $k \in \mathbb{N}$ ein $m(k) \in \mathbb{N}$ existiert, so daß jede natürliche Zahl Summe von höchstens $m(k)$ k-ten Potenzen ist?
Die positive Antwort gab Hilbert (1862 - 1943) im Jahre 1909. Damit war die weitergehende Frage nach dem kleinsten $m(k)$, genannt $g(k)$, sinnvoll. Schon Euler hatte die Ungleichung

$$g(k) \geq \left[\left(\frac{3}{2}\right)^k\right] + 2^k - 2 =: h(k)$$

gezeigt. Man vermutet $g(k) = h(k)$, und man weiß seit 1957, daß diese Formel für höchstens endlich viele k falsch sein kann (Mahler, 1903-1988). Einzelergebnisse stammen etwa von

Lagrange (1770):	$g(2) = 4$,
Wieferich (1909):	$g(3) = 9$,
Balasubramanian, Deshouillers, Dress (1985):	$g(4) = 19$,
Chen (1964):	$g(5) = 37$,
Pillai (1940):	$g(6) = 73$.

Beispiel 8. Das Partitionenproblem von Hardy (1877 - 1947) und Ramanujan (1887 - 1920) lautet: Wieviele Zerlegungen von $n \in \mathbb{N}$ in natürliche Summanden gibt es (dabei seien die Summanden etwa der Größe nach geordnet)? Wird die gesuchte Anzahl mit $p(n)$ bezeichnet, so ergibt sich für $n = 4$ zum Beispiel:

$$\left.\begin{array}{l} 4 \\ 3+1 \\ 2+2 \\ 2+1+1 \\ 1+1+1+1 \end{array}\right\} \quad p(4) = 5.$$

Hardy und Ramanujan bewiesen 1918 mit analytischen Methoden ihre berühmte Partitionenformel

$$p(n) \sim \frac{1}{4n\sqrt{3}}\, e^{\pi\sqrt{\frac{2n}{3}}} \qquad (n \to \infty).$$

Beispiel 9. Schon bei Euklid steht mit Beweis: Es gibt unendlich viele Primzahlen. In der Neuzeit hat die Frage nach der Verteilung der Primzahlen eine bedeutende Rolle gespielt. Bezeichnet $\pi(x)$ die Anzahl der Primzahlen $\leq x$, so gilt der u. a. von Gauss vermutete Primzahlsatz

$$\pi(x) \sim \frac{x}{\log x} \qquad (x \to \infty).$$

Der erste Beweis wurde 1896 unabhängig voneinander durch Hadamard (1865 - 1963) und de la Vallée Poussin (1866-1962) erbracht. Er verwendet tiefe funktionentheoretische Hilfsmittel zum Nachweis spezieller Eigenschaften der (zunächst nur für $\operatorname{Re} s > 1$ definierten) Riemannschen Zeta-Funktion (Riemann, 1826 - 1866)

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

die sich analytisch auf die ganze komplexe Ebene fortsetzen läßt mit Ausnahme eines einfachen Pols bei $s = 1$. Die Primzahlverteilung korrespondiert nun mit der Lage der komplexen Nullstellen von $\zeta(s)$ im Streifen $0 < \operatorname{Re} s < 1$. Die berühmte Riemannsche Vermutung besagt, daß alle diese Nullstellen den Realteil $\frac{1}{2}$ besitzen. Sie ist bis heute unbewiesen. Ihre Richtigkeit hätte die Konsequenz

$$\pi(x) = \operatorname{li}(x) + R(x)$$

mit dem Integrallogarithmus

$$\operatorname{li}(x) = \int_e^x \frac{dt}{\log t}$$

und dem Restglied

$$R(x) = \mathcal{O}\big(\sqrt{x}\,\log x\big).$$

Die bis heute beste Restgliedabschätzung

$$R(x) = \mathcal{O}\left(x\,\exp\left(-\,c\,\frac{(\log x)^{3/5}}{(\log\log x)^{1/5}}\right)\right)$$

mit einer positiven Konstanten c stammt von Vinogradov (1891 - 1983) aus dem Jahre 1958. Es gibt inzwischen mehrere verschiedene Beweise des Primzahlsatzes, darunter auch einen 1947 zur Überraschung der Fachwelt gefundenen elementaren Beweis von Erdös (1913 - 1986) und Selberg.

Beispiel 10. Bis heute offen ist das Primzahlzwillingsproblem: Gibt es unendlich viele Primzahlpaare $p, p+2$? Man weiß seit 1919, daß die Reihe

$$\sum_{\substack{p \text{ prim} \\ p+2 \text{ prim}}} \frac{1}{p}$$

konvergiert (Brun, 1885 - 1978), während die Reihe über die reziproken Primzahlen bekanntlich divergiert.

Bis heute ungeklärt ist auch die Frage: Gibt es unendlich viele Primzahlen der Form n^2+1? Man weiß mit Hilfe scharfsinniger Siebmethoden, daß unendlich viele dieser Zahlen entweder Primzahlen oder Produkte von zwei Primzahlen sind (Iwaniec, 1978).
Dirichlet (1805 - 1859), Nachfolger von Gauß in Göttingen und Begründer der analytischen Zahlentheorie, bewies, daß in jeder arithmetischen Progression $a, a+q, a+2q, \ldots$ mit teilerfremden Zahlen $a, q \in \mathbb{N}$ unendlich viele Primzahlen liegen.

Beispiel 11. In einem Brief an Euler stellte Goldbach 1742 die folgende Vermutung auf:

a) Jede gerade natürliche Zahl $n \geq 4$ ist Summe von zwei Primzahlen.

Hieraus folgt sofort:

b) Jede ungerade natürliche Zahl $n \geq 7$ ist Summe von drei Primzahlen.

Ist nämlich $n \geq 7$ ungerade, so ist $n-3 \geq 4$ gerade, und man hat nach a) dann $n = 3+p+p'$ mit Primzahlen p, p'. Die Vermutung a) erscheint auch heute noch nicht angreifbar. Immerhin weiß man durch Chen seit 1973, daß jedes gerade $n \geq 4$ Summe $p+p_2$ aus einer Primzahl und einer Zahl mit höchstens zwei Primfaktoren ist. Der Beweis verwendet wieder Siebmethoden. Die Vermutung b) ist dagegen im wesentlichen gelöst. Vinogradov zeigte 1937 mit raffinierten Abschätzungen von Exponentialsummen, daß jede hinreichend große ungerade natürliche Zahl Summe von drei Primzahlen ist. Ein wesentliches Hilfsmittel ist die 1923 entwickelte Hardy-Littlewoodsche Kreismethode (Littlewood,1885 - 1977).

Beispiel 12. Zwei Gitterpunktprobleme sind

a) das Gaußsche Kreisproblem: Gesucht ist die Anzahl $A(x)$ der Paare $(a,b) \in \mathbb{Z}^2$ mit $a^2+b^2 \leq x$,

b) das Dirichletsche Teilerproblem: Gesucht ist die Anzahl $B(x)$ der Paare $(a,b) \in \mathbb{N}^2$ mit $ab \leq x$.

Verhältnismäßig leicht zu sehen sind die Abschätzungen

$$A(x) - \pi\, x \ll x^{\frac{1}{2}}\,, \quad B(x) - x\, \log x - (2\gamma - 1)\, x \ll x^{\frac{1}{2}}$$

mit der Euler-Mascheroni Konstante

$$\gamma = \lim \Big(\sum_{1 \leq \nu \leq n} \frac{1}{\nu} - \log\, n \Big).$$

Es entsteht die Frage, für welche Exponenten ϑ die obigen Abschätzungen mit x^{ϑ} anstelle von $x^{\frac{1}{2}}$ zutreffen. Für $\lambda = \inf \vartheta$ ist durch Hardy und Landau (1877 - 1938) jeweils bekannt

$$\frac{1}{4} \leq \lambda < \frac{1}{3}\,.$$

Es gibt Verbesserungen der oberen Schranke.

1.2 Versuch einer Gliederung

Es folgt ein grober Überblick über zentrale Teilgebiete der Zahlentheorie.

A) Elementare Zahlentheorie
Teilbarkeitstheorie, ganzzahlige Lösungen von Gleichungen und Ungleichungen, elementare Primzahltheorie. Elementare Hilfsmittel, d. h. ohne komplexe Analysis. (Beispiele 1, 2, 6)

B) Algebraische Zahlentheorie
Zahlentheorie in abstrakten Zahlbereichen (wie $\mathbb{Z}[i]$ oder $\mathbb{Z}[\sqrt{2}]$). Algebraische Methoden und Methoden der algebraischen Geometrie (rationale Punkte auf algebraischen Kurven). (Beispiele 3, 4, 5)

C) Analytische Zahlentheorie
Anwendung funktionentheoretischer Methoden. (Beispiele 8, 9, 10, 11, 12)

D) Diophantische Approximation und Transzendenztheorie
Kettenbrüche, Approximation von reellen durch rationale Zahlen (etwa sind $\frac{3}{1}$, $\frac{22}{7}$, $\frac{355}{113}$ „beste“ Approximationen von π); Transzendenzbeweise von e durch Hermite (1822 - 1901) im Jahr 1873, von π durch Lindemann im Jahr 1882, von α^β für algebraische Zahlen $\alpha \notin \{0, 1\}, \beta$ durch Gelfond und Schneider unabhängig voneinander im Jahre 1934. Bis heute ist aber unbekannt, ob zum Beispiel γ irrational oder gar transzendent ist. (Beispiel 3)

E) Multiplikative Zahlentheorie
Primzahlprobleme, Exponentialsummen, Siebmethoden usw. (Beispiele 8, 9)

F) Additive Zahlentheorie
Summe von Zahlenfolgen usw. Entwicklung dieser Theorie seit etwa 1933 durch Schnirelmann, Erdös u.a. (Beispiele 5, 6, 7, 8)

G) Probabilistische Zahlentheorie
Methoden der Wahrscheinlichkeitstheorie, angewandt auf Verteilungsfragen bei Zahlenfolgen usw. Entwicklung seit etwa 1934 durch Turán, Erdös, Rényi, Kubilius u.a.

H) Algorithmische Zahlentheorie
Rechnergestützte zahlentheoretische Algorithmen, zum Beispiel Primzahltests, Faktorisierungsmethoden, Anwendungen der Fast Fourier Transform usw. Entwicklung seit etwa 1935 (!) durch Lehmer, ab etwa 1970 durch Lenstra und Lenstra, Pollard, Adleman u. a.

Diese Einteilung ist nicht streng.

1.3 Aufgaben und Lösungen

In den nachstehenden Aufgaben und Lösungen werden Begriffe wie Teiler, Primzahl usw. als bekannt vorausgesetzt; ihre Eigenschaften werden in Kapitel 2 systematisch entwickelt.

Aufgabe 1. Man finde notwendige Bedingungen an $k \in \mathbb{N}$ derart, daß $2^k \pm 1$ prim ist.

Lösung: Mit $\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, \dots\}$ bezeichnen wir die Menge der Primzahlen. Es gilt:

(a) Aus $2^k - 1 \in \mathbb{P}$ folgt $k \in \mathbb{P}$;
(b) Aus $2^k + 1 \in \mathbb{P}$ folgt $k = 2^m$ mit $m \in \mathbb{N}_0$.

Der Nachweis verwendet in beiden Fällen die geometrische Summe

$$q^n - 1 = (q-1)(q^{n-1} + \cdots + q + 1).$$

Aus der Annahme $k = dm$ mit natürlichen Zahlen $d \neq 1$, $m \neq 1$ bzw. $k = 2^m u$ mit $m \in \mathbb{N}_0$ und ungeradem $u \in \mathbb{N}$, $u \neq 1$, folgt jeweils ein Widerspruch. Die Primzahlen der Form $2^p - 1$ heißen Mersennesche Primzahlen (vgl. Beispiel 2), die der Form $2^{2^m} + 1$ Fermatsche Primzahlen (vgl. Beispiel 4).

Aufgabe 2. Man zeige die Sätze von Euklid und Euler: Genau dann ist die gerade Zahl $n \in \mathbb{N}$ vollkommen, wenn $n = 2^k(2^{k+1} - 1)$ mit einer Mersenneschen Primzahl $2^{k+1} - 1$ gilt.

Lösung: Es ist zweckmäßig, die Teilersummenfunktion $\sigma : \mathbb{N} \to \mathbb{N}$ einzuführen. Man definiert

$$\sigma(n) = \sum_{d|n} d \qquad (n \in \mathbb{N})$$

als die Summe aller natürlichen Teiler d von n. Offenbar ist $n \in \mathbb{N}$ genau dann vollkommen, wenn $\sigma(n) = 2n$ gilt. Die Werte von σ sind ziemlich unregelmäßig verteilt. Eine wichtige Eigenschaft der arithmetischen Funktion σ ist ihre Multiplikativität,

$$\sigma(mn) = \sigma(m)\,\sigma(n) \quad \text{für alle teilerfremden } m, n \in \mathbb{N}.$$

Denn alle natürlichen Teiler von mn kommen genau einmal unter den Produkten aller natürlichen Teiler von m mit allen natürlichen Teilern von n vor. Man sieht $\sigma(p^\nu) = 1+p+p^2+\cdots+p^\nu$ für $p \in \mathbb{P}$ und $\nu \in \mathbb{N}$.
Zum Nachweis des Satzes von Euklid sei $p = 2^{k+1} - 1 \in \mathbb{P}$. Dann sind p und 2^k teilerfremd, und mit $n = 2^k p$ gilt

$$\sigma(n) = \sigma(2^k)\,\sigma(p) = (1 + 2 + \cdots + 2^k)(p+1) = (2^{k+1} - 1)2^{k+1} = 2n\,,$$

was zu zeigen war.

Zum Nachweis des Satzes von Euler sei $n = 2^k m$ mit $k, m \in \mathbb{N}$, m ungerade, eine vollkommene Zahl, also

$$(2^{k+1} - 1)\,\sigma(m) = 2^{k+1} m\,.$$

Da 2^{k+1} und $2^{k+1} - 1$ teilerfremd sind, muß 2^{k+1} ein Teiler von $\sigma(m)$ sein. Das heißt

$$\lambda := \frac{\sigma(m)}{2^{k+1}} = \frac{m}{2^{k+1} - 1} \in \mathbb{N}.$$

Angenommen, es besteht $\lambda > 1$. Dann folgt

$$\sigma(m) = \sigma(\lambda(2^{k+1} - 1)) > \lambda(2^{k+1} - 1) + \lambda = \lambda\, 2^{k+1} = \sigma(m)\,,$$

was unmöglich ist. Daher gilt $\lambda = 1$, also $m = 2^{k+1} - 1$. Ist nun m nicht Primzahl, so folgt $\sigma(m) > 2^{k+1} = \sigma(m)$, was nicht sein kann. Daher ist notwendig $n = 2^k(2^{k+1} - 1)$ mit $2^{k+1} - 1 \in \mathbb{P}$ (vgl. Beispiel 2).

Aufgabe 3. Man bestimme alle Lösungstripel $(x, y, z) \in \mathbb{N}^3$ von $x^2 + y^2 = z^2$.

Lösung: Mit $\xi = \frac{x}{z}$ und $\eta = \frac{y}{z}$ sind die rationalen Punkte $(\xi, \eta) \in \mathbb{Q}^2$ mit $\xi, \eta > 0$ auf dem Einheitskreis E: $\xi^2 + \eta^2 = 1$ zu bestimmen. Wir parametrisieren E im ersten Quadranten durch die Schnittpunktkoordinaten der Geraden $\eta = t(\xi + 1)$ mit dem Kreis E für $0 < t < 1$. Es folgt

$$\xi = \frac{1 - t^2}{1 + t^2}, \quad \eta = \frac{2t}{1 + t^2} \qquad (0 < t < 1).$$

Damit ξ, η rational sind, muß $t = \frac{1-\xi}{\eta}$ rational sein. Es sei also $t = \frac{m}{n}$ mit teilerfremden $m, n \in \mathbb{N}$ und $m < n$. Dann folgt $\xi = \frac{n^2-m^2}{n^2+m^2}$, $\eta = \frac{2mn}{n^2+m^2}$ und daraus

$$x = d(n^2 - m^2), \quad y = 2dmn, \quad z = d(m^2 + n^2)$$

mit teilerfremden $m, n \in \mathbb{N}$, $m < n$, und $d \in \mathbb{N}$, bis auf Vertauschung von x, y (vgl. Beispiel 1).

Aufgabe 4. Es seien $g, k \in \mathbb{N}$ fest, und jedes $n \in \mathbb{N}$ besitze eine Darstellung $n = n_1^k + \cdots + n_g^k$ mit $n_1, \ldots, n_g \in \mathbb{N}_0$. Man beweise die Eulersche Abschätzung

$$g \geq \left[\left(\frac{3}{2}\right)^k\right] + 2^k - 2.$$

Lösung: Die natürliche Zahl

$$n = \left(\left[\left(\frac{3}{2}\right)^k\right] - 1\right)2^k + (2^k - 1)1^k$$

ist kleiner als 3^k. In der Darstellung von n als Summe von k-ten Potenzen kommen daher nur die Summanden 2^k und 1^k vor. Die kürzeste Darstellung erfordert offenbar $\left[\left(\frac{3}{2}\right)^k\right] - 1$ Summanden 2^k und $2^k - 1$ Summanden 1^k. Das ergibt die Behauptung (vgl. Beispiel 7).

Aufgabe 5. Man beweise den Satz von Euklid, daß es unendlich viele Primzahlen gibt.

Lösung: Es sei $T \subseteq \mathbb{P}$ eine nichtleere, endliche Menge und

$$n = \prod_{p \in T} p + 1.$$

Dann gilt $n > 1$, und n besitzt eine Primfaktorzerlegung, in der jedenfalls keine Primzahl aus T vorkommt. Es gibt daher eine Primzahl $q \notin T$. Daraus folgt die Behauptung (vgl. Beispiel 9).

In derselben Weise sieht man auch, daß es unendlich viele Primzahlen gibt, die bei Division durch 4 den Rest 3 lassen. Etwa betrachte man

$$n = 4 \prod_{p \in T} p - 1.$$

Es erfordert aber bereits neue Ideen, die Unendlichkeit der Menge der Primzahlen von der Form $4m + 1$ mit $m \in \mathbb{N}$ zu zeigen.

Aufgabe 6. Es sei $A(x)$ die Anzahl der Zahlenpaare $(a, b) \in \mathbb{Z}^2$ mit $a^2 + b^2 \leq x$ für $x \geq 2$. Man zeige die Existenz einer Konstanten $c > 0$ mit

$$|A(x) - \pi\, x| \leq c\,\sqrt{x}\,.$$

Lösung: Jedem Gitterpunkt $(a, b) \in \mathbb{Z}^2$ der Ebene sei das Einheitsquadrat des Gitters mit der linken unteren Ecke (a, b) zugeordnet. Diese Abbildung ist bijektiv. Die Diagonale im Einheitsquadrat hat die Länge $\sqrt{2}$. Wir betrachten die Kreise vom Radius $\sqrt{x} - \sqrt{2}$, $\sqrt{x}$, $\sqrt{x}+\sqrt{2}$ um den Nullpunkt. Ein Flächenvergleich ergibt $\pi \left(\sqrt{x}-\sqrt{2}\right)^2 \leq A(x) \leq \pi \left(\sqrt{x}+\sqrt{2}\right)^2$. Es folgt

$$|A(x) - \pi\, x| \leq 2\sqrt{2}\,\pi\sqrt{x} + 2\,\pi \leq 3\sqrt{2}\,\pi\,\sqrt{x}\,,$$

wie behauptet (vgl. Beispiel 12).

Kapitel 2

Der Euklidische Algorithmus

Dieser Kapitel behandelt Teilbarkeitstheorie in $\mathbb{Z}$ und verwendet sie zur Lösung linearer diophantischer Gleichungen.

2.1 Teilbarkeit

Die Mengen $\mathbb{N}$, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sind wie üblich erklärt, und $\mathbb{Z}^\times$, $\mathbb{Q}^\times$, $\mathbb{R}^\times$, $\mathbb{C}^\times$ bezeichnen die entsprechenden Mengen ohne die Null.

Definition. Es sei $a \in \mathbb{Z}^\times$, $b \in \mathbb{Z}$. Man nennt a Teiler von b (b Vielfaches von a), in Zeichen $a \mid b$, wenn es ein $\lambda \in \mathbb{Z}$ mit $b = \lambda a$ gibt. Ist a nicht Teiler von b, so schreibt man $a \nmid b$.

Folgerung 1. Es gelten die folgenden Aussagen:

a) Die Teiler von b und $-b$ stimmen überein; mit a ist auch $-a$ Teiler von b. Für $a \in \mathbb{Z}^\times$ gilt stets $a \mid 0$ und $1 \mid a$.

b) Die Teilbarkeitsbeziehung ist reflexiv und transitiv: Für $a, b \in \mathbb{Z}^\times$ gilt $a \mid a$, und aus $a \mid b$ und $b \mid c$ folgt $a \mid c$. Sie ist im allgemeinen nicht symmetrisch; aber $a \mid b$ und $b \mid a$ impliziert $a = \pm b$.

c) Aus $a \mid c$ und $a \mid d$ folgt $a \mid (cx + dy)$ für alle $x, y \in \mathbb{Z}$.

Satz 1. (Division mit Rest) Zu $a \in \mathbb{Z}$, $b \in \mathbb{N}$ existieren eindeutig bestimmte $q, r \in \mathbb{Z}$ mit

$$a = qb + r \quad \text{und} \quad 0 \leq r < b$$

Bezeichnet $[x]$ für $x \in \mathbb{R}$ die größte ganze Zahl $\leq x$, so gilt $q = \left[\frac{a}{b}\right]$ und $r = a - \left[\frac{a}{b}\right] b$.

Beweis. Unter den Zahlen $a - nb$ mit $n \in \mathbb{Z}$ kommen negative und nichtnegative vor. Die kleinste nichtnegative Zahl dieser Art sei $r = a - qb$. Das heißt, es gilt $r \geq 0$ und $r - b =$

$a-(q+1)b<0$. Es folgt $a=qb+r$ mit $0\le r<b$. Die Eindeutigkeit kommt aus $\frac{a}{b}=q+\frac{r}{b}$ mit $0\le\frac{r}{b}<1$, also $q=\left[\frac{a}{b}\right]$, $r=a-\left[\frac{a}{b}\right]b$. □

Satz 2. Es seien $a,b\in\mathbb{Z}$ nicht beide Null. Dann existiert eine eindeutig bestimmte Zahl $d\in\mathbb{Z}$ mit

a) $d>0$;

b) $d\mid a$ und $d\mid b$,

c) aus $t\mid a$ und $t\mid b$ folgt $t\mid d$.

Beweis. Die Eindeutigkeit ergibt sich so: Sind $d,d'\in\mathbb{Z}$ zwei Zahlen mit den Eigenschaften a), b), c), so gilt $d\mid d'$ und $d'\mid d$ wegen c) sowie $d,d'\in\mathbb{N}$. Folgerung 1 b) liefert $d=d'$.

Da für $b=0$ offenbar $d=|a|$ die gewünschten Eigenschaften a), b), c) besitzt, genügt es wegen Folgerung 1 a) den Existenzbeweis für $a,b\in\mathbb{N}$ zu führen. Es sei etwa $a\ge b$. Sukzessive Division mit Rest liefert das nachstehende Schema:

$$\begin{aligned}
a &= q_1 b &&+ r_1\,, && 0<r_1<b &\quad,\\
b &= q_2 r_1 &&+ r_2\,, && 0<r_2<r_1 &\quad,\\
r_1 &= q_3 r_2 &&+ r_3\,, && 0<r_3<r_2 &\quad,\\
&\vdots\\
r_{k-2} &= q_k r_{k-1} &&+ r_k\,, && 0<r_k<r_{k-1}\,,\\
r_{k-1} &= q_{k+1} r_k\,. &&
\end{aligned}$$

Das Divisionsverfahren wird also solange durchgeführt, bis der Rest r_{k+1} erstmals verschwindet. Die Existenz eines solchen $k\in\mathbb{N}_0$ ist klar, weil die Reste $r_1,r_2,\dots$ eine streng monoton fallende Folge von nichtnegativen ganzen Zahlen bilden. Der Divisionsprozeß bricht daher ab.

Liest man das Schema rückwärts, so sieht man $r_k\mid r_{k-1}$, $r_k\mid r_{k-2},\dots,r_k\mid b$, $r_k\mid a$. Daher ist r_k gemeinsamer Teiler von a,b. Ist nun t irgendein gemeinsamer Teiler von a,b, so sieht man, indem man das Schema vorwärts liest, $t\mid r_1$, $t\mid r_2,\dots,t\mid r_k$. Also erfüllt die Zahl $d=r_k$ die Bedingungen a), b), c). □

Definition. Die Zahl d aus Satz 2 heißt der größte gemeinsame Teiler (kurz: ggT, englisch: gcd) von a und b, in Zeichen: $d=(a,b)$ oder $d=\mathrm{ggT}(a,b)$.
Das im Beweis von Satz 2 durchgeführte Verfahren der sukzessiven Division mit Rest ist der Euklidische Algorithmus.

Beispiel 1. Für $a=31\,031$, $b=10\,013$ ergibt sich $\mathrm{ggT}(31\,031,10\,013)=31$ aus

$$\begin{aligned}
31\,031 &= 3\cdot 10\,013 &&+ 992\\
10\,013 &= 10\cdot 992 &&+ 93\\
992 &= 10\cdot 93 &&+ 62\\
93 &= 1\cdot 62 &&+ 31\\
62 &= 2\cdot 31
\end{aligned}$$

Definition. Gilt $(a,b)=1$, so heißen die Zahlen a,b teilerfremd (relativ prim).

Folgerung 2. Es gelten die nachstehenden Rechenregeln:

a) Für $m \neq 0$ gilt stets $(ma, mb) = m\,(a, b)$.

b) Gilt $m \mid a$ und $m \mid b$, so besteht $\left(\frac{a}{m}\,,\ \frac{b}{m}\right) = \frac{1}{m}\,(a, b)$.

c) Gilt $(a, b) = d$, so existieren $x, y \in \mathbb{Z}$ mit $d = ax + by$; sind speziell $a, b \in \mathbb{Z}$ teilerfremd, so existieren $x, y \in \mathbb{Z}$ mit $1 = ax + by$, und umgekehrt.

d) Aus $(a, b) = (a, c) = 1$ folgt $(a, bc) = 1$.

e) Aus $a \mid bc$ und $(a, b) = 1$ folgt $a \mid c$.

Nachweis. a) Man führe den Euklidischen Algorithmus für a, b und für ma, mb durch. b) Man schreibe $a = ma'$, $b = mb'$ und verwende a). c) Löst man die Gleichungen des Euklidischen Algorithmus rückwärts nach $d = r_k$ auf, so erweist sich d als Linearkombination der Zahlen a, b mit ganzen Koeffizienten. Daraus und aus Folgerung 1 c) kommt der Zusatz. d) Man hat $1 = ax + by$, $1 = ax' + by'$ mit $x, x', y, y' \in \mathbb{Z}$, also auch $1 = (ax + by)(ax' + by') = a(axx' + cxy' + bx'y) + bc(yy')$. Die beiden Klammerausdrücke sind jeweils ganz, mit Folgerung c) ergibt sich $(a, bc) = 1$. e) Wegen $1 = ax + by$ mit $x, y \in \mathbb{Z}$ gilt $c = acx + bcy$, und aus $a \mid ac$, $a \mid bc$ sowie Folgerung 1 c) kommt $a \mid c$. □

Beispiel 2. Aus Beispiel 1 folgt

$$\begin{aligned} 31 &= 93 - 1 \cdot 62 = 93 - 1 \cdot (992 - 10 \cdot 93) = 11 \cdot 93 - 1 \cdot 992 \\ &= 11 \cdot (10\,013 - 10 \cdot 992) - 1 \cdot 992 = 11 \cdot 10\,013 - 111 \cdot 992 \\ &= 11 \cdot 10\,013 - 111 \cdot (31\,031 - 3 \cdot 10\,013) \\ &= 344 \cdot 10\,013 - 111 \cdot 31\,031 \\ &= 344b - 111a\,. \end{aligned}$$

Satz 3. Es seien $a, b \in \mathbb{Z}^\times$. Dann existiert eine eindeutig bestimmte Zahl $m \in \mathbb{Z}$ mit

a) $m > 0$,

b) $a \mid m$ und $b \mid m$,

c) aus $a \mid v$ und $b \mid v$ folgt $m \mid v$.

Beweis. Die Eindeutigkeit wird wie in Satz 2 erledigt.

Die Existenz ergibt sich, indem man für $m = \frac{|ab|}{(a,b)}$ die behaupteten Eigenschaften verifiziert: a) ist klar; b) folgt aus $(a, b) \mid b$, $m = |a| \cdot \frac{|b|}{(a,b)}$, sowie aus $(a, b) \mid a$, $m = |b| \cdot \frac{|a|}{(a,b)}$. c) Wegen Folgerung 2 c) existieren $x, y \in \mathbb{Z}$ mit $(a, b) = |a|x + |b|y$. Daraus folgt

$$v = \frac{v}{(a, b)}\,(a, b) = \frac{v}{(a, b)}\,(|a|x + |b|y) = m\Big(\frac{v}{|b|}\,x + \frac{v}{|a|}\,y\Big),$$

worin der Klammerausdruck wegen $a \mid v$, $b \mid v$ ganzzahlig ist, also $m \mid v$. □

Definition. Die Zahl m aus Satz 3 heißt das kleinste gemeinschaftliche Vielfache (kurz: kgV, englisch: lcm) von a und b, in Zeichen: $[a, b]$ oder $\mathrm{kgV}[a, b]$.

Folgerung 3. Für $a, b \in \mathbb{Z}^\times$ gilt $(a, b) \cdot [a, b] = |ab|$.

2.2 Primfaktorzerlegung

Definition. Es sei $1 \neq p \in \mathbb{N}$. Besitzt p nur 1 und p als natürliche Teiler, so heißt p Primzahl. Die Menge der Primzahlen $2, 3, 5, \ldots$ wird mit $\mathbb{P}$ bezeichnet.

Bemerkung 1. Primzahlen werden durchweg mit dem Buchstaben p bezeichnet. Das leere Produkt hat vereinbarungsgemäß den Wert 1.

Satz 4. (Fundamentalsatz der Zahlentheorie) Jede natürliche Zahl ist Produkt von Primzahlen. Die Darstellung ist, abgesehen von der Reihenfolge der Faktoren, eindeutig.

Beweis. Existenz: Für $n = 1, 2$ ist die Behauptung wahr. Sie treffe schon zu für alle $n < k$. Dann ist entweder k Primzahl, oder k hat einen echten Teiler $\ell \in \mathbb{N}$. Im letzten Fall besteht $k = \ell\, m$ mit $\ell, m \in \mathbb{N}$, $1 < \ell, m < k$. Da nach Induktionsvoraussetzung ℓ, m Primzahlprodukte sind, ist auch $k = \ell\, m$ Produkt von Primzahlen.

Eindeutigkeit (Zermelo, 1871 - 1953): Der Fall $n = 1$ ist klar. Angenommen, es gibt natürliche Zahlen > 1 mit verschiedenen Primfaktorzerlegungen. Es sei $n \in \mathbb{N}$ die kleinste von ihnen. Dann hat man $n = pm = p'm'$ mit verschiedenen Primzahlen $p < p'$ und $m, m' \in \mathbb{N}$, $m, m' > 1$, $p \nmid m'$. Man betrachte die Zahl

$$k = n - pm' = p(m - m') = (p' - p)m'.$$

Offenbar gilt $1 < k < n$. Nach Voraussetzung ist die Primfaktorzerlegung von k eindeutig. Es folgt $p \mid (p' - p)m'$. Da p nicht in m' aufgeht, gilt $p \mid (p' - p)$, also $p \mid p'$. Dies ist für verschiedene Primzahlen unmöglich. □

Folgerung 4. Es gelten die folgenden Aussagen.

a) Jedes $n \in \mathbb{N}$ besitzt eine kanonische Darstellung als Produkt von Primzahlpotenzen $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ mit Primzahlen $p_1 < \ldots < p_r$ und Exponenten $\nu_1, \ldots, \nu_r \in \mathbb{N}$. Diese Darstellung ist eindeutig.

b) Aus $p, p_1, \ldots, p_r \in \mathbb{P}$ und $p \mid p_1 \cdots p_r$ folgt $p = p_\varrho$ für ein ϱ mit $1 \leq \varrho \leq r$.

Folgerung 5. Besitzen $a, b \in \mathbb{Z}^\times$ die kanonischen Darstellungen

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

so gilt

$$(a, b) = \prod_p p^{\min\{\alpha_p, \beta_p\}}, \quad [a, b] = \prod_p p^{\max\{\alpha_p, \beta_p\}}.$$

Nachweis. Man setze

$$d = \prod_p p^{\min\{\alpha_p, \beta_p\}}.$$

Es gilt $d > 0$ sowie $d \mid a$ und $d \mid b$, also $d \mid (a, b)$. Weiter gilt

$$\alpha_p - \min\{\alpha_p, \beta_p\} = 0 \quad \text{oder} \quad \beta_p - \min\{\alpha_p, \beta_p\} = 0$$

für jedes $p \in \mathbb{P}$. Daher sind $\frac{|a|}{d}$, $\frac{|b|}{d} \in \mathbb{N}$ teilerfremd. Es folgt $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ oder $(a,b) = d$ gemäß Folgerung 2 b).

Die zweite Behauptung kommt aus Folgerung 3,

$$[a,b] = \frac{|ab|}{(a,b)} = \prod_p p^{\alpha_p+\beta_p-\min\{\alpha_p,\beta_p\}} = \prod_p p^{\max\{\alpha_p,\beta_p\}}.$$

□

Definition. Es seien $a_1, \ldots, a_r \in \mathbb{Z}^\times$ mit $a_\varrho = \pm\prod_p p^{\alpha_{\varrho p}}$ für $\varrho = 1, \ldots, r$. Dann heißen

$$(a_1, \ldots, a_r) = \prod_p p^{\min\{\alpha_{1p},\ldots,\alpha_{rp}\}} \quad \text{der ggT von } a_1, \ldots, a_r,$$
$$[a_1, \ldots, a_r] = \prod_p p^{\max\{\alpha_{1p},\ldots,\alpha_{rp}\}} \quad \text{das kgV von } a_1, \ldots, a_r.$$

Folgerung 6. Der ggT und das kgV der Zahlen $a_1, \ldots, a_r \in \mathbb{Z}^\times$ haben die folgenden Eigenschaften:

a) $(a_1, \ldots, a_r) > 0$, $[a_1, \ldots, a_r] > 0$,

b) $(a_1, \ldots, a_r) \mid a_\varrho$ für $1 \le \varrho \le r$, $a_\varrho \mid [a_1, \ldots, a_r]$ für $1 \le \varrho \le r$,

c) aus $t \mid a_\varrho$ $(1 \le \varrho \le r)$ folgt $t \mid (a_1, \ldots, a_r)$,
aus $a_\varrho \mid v$ $(1 \le \varrho \le r)$ folgt $[a_1, \ldots, a_r] \mid v$.

Ferner gilt $(a_1, a_2, a_3) = (a_1, (a_2, a_3))$, $[a_1, a_2, a_3] = [a_1, [a_2, a_3]]$ usw.

2.3 Lineare diophantische Gleichungen

Unter diophantischen Gleichungen versteht man Polynomgleichungen mit ganzzahligen Koeffizienten, an deren ganzzahligen Lösungen Interesse besteht (Diophant, ca. 250 n.Chr.). Hier wollen wir notwendige und hinreichende Bedingungen für die ganzzahlige Lösbarkeit der Gleichung

$$(*) \qquad ax + by = c \qquad (a, b, c \in \mathbb{Z} \text{ fest}; a, b \text{ nicht beide Null})$$

sowie die allgemeine Lösung von $(*)$ in ganzen Zahlen x, y bestimmen.

Satz 5. Notwendige und hinreichende Bedingung für die ganzzahlige Lösbarkeit von $(*)$ ist die Bedingung $(a,b) \mid c$. Ist x_0, y_0 eine ganzzahlige Lösung von $(*)$, so sind alle Lösungen $x, y \in \mathbb{Z}$ von $(*)$ gegeben durch

$$x = x_0 + \frac{b}{(a,b)}\,t, \quad y = y_0 - \frac{a}{(a,b)}\,t \qquad (t \in \mathbb{Z}).$$

Beweis. Die Bedingung $(a,b) \mid c$ ist notwendig. Sie ist auch hinreichend, denn aus der Teilerfremdheit von $\frac{a}{(a,b)}$, $\frac{b}{(a,b)} \in \mathbb{Z}$ folgt die Existenz von $x', y' \in \mathbb{Z}$ mit

$$1 = \frac{a}{(a,b)}\, x' + \frac{b}{(a,b)}\, y', \quad \text{also } c = \frac{ac}{(a,b)}\, x' + \frac{bc}{(a,b)}\, y'.$$

Demnach sind

$$x_0 = \frac{c}{(a,b)}\, x', \quad y_0 = \frac{c}{(a,b)}\, y'$$

Lösungen von $(*)$. Ist $x, y \in \mathbb{Z}$ eine weitere Lösung von $(*)$, so entsteht durch Differenzbildung $a(x - x_0) + b(y - y_0) = 0$, also

$$\frac{a}{(a,b)}\,(x - x_0) = -\frac{b}{(a,b)}\,(y - y_0).$$

Da $\frac{a}{(a,b)}$ und $\frac{b}{(a,b)}$ teilerfremd sind, folgt notwendig

$$x - x_0 = t\,\frac{b}{(a,b)}, \quad y - y_0 = -t\,\frac{a}{(a,b)} \qquad (t \in \mathbb{Z}).$$

Einsetzen zeigt, daß dies wirklich Lösungen von $(*)$ sind. □

Beispiel 3. Es sei $a = 31\,031$, $b = 10\,013$, $c = 1\,736$. Die diophantische Gleichung $ax + by = c$ ist wegen $(a,b) = 31$ und $1736 = 31 \cdot 56$ lösbar. Beispiel 2 liefert als eine spezielle Lösung: $x_0 = -111 \cdot 56$, $y_0 = 344 \cdot 56$. Also lautet die allgemeine Lösung

$$x = -111 \cdot 56 + 323\,t, \quad y = 344 \cdot 56 - 1001\,t \qquad (t \in \mathbb{Z}).$$

In vielen Fällen, etwa bei kleinen Koeffizienten a, b, c läßt sich eine spezielle Lösung x_0, y_0 von $(*)$ durch Raten ermitteln. Der Euklidische Algorithmus führt stets zum Ziel.

Für $d \in \mathbb{Z}^\times$ stimmen die Lösungsgesamtheiten von $ax + by = c$ und von $adx + bdy = cd$ überein. Es brauchen daher nur reduzierte diophantische Gleichungen $(*)$ mit $(a,b) = 1$ gelöst zu werden. Lineare Diophantische Gleichungen mit mehr als zwei Variablen lassen sich entsprechend behandeln.

Kapitel 3

Restklassenringe

In diesem Kapitel wird das Studium der Teilbarkeit fortgesetzt, und zwar im Rahmen der Kongruenztheorie, die von Gauß 1801 in den *Disquisitiones Arithmeticae* systematisch entwickelt wurde.

3.1 Definition und grundlegende Eigenschaften

Definition. Es seien $a, b \in \mathbb{Z}$, $q \in \mathbb{N}$. Gilt $q \mid (b-a)$, so heißen a, b kongruent modulo q, in Zeichen: $a \equiv b \bmod q$ oder auch $a \equiv b(q)$.

Satz 1. Genau dann gilt $a \equiv b \bmod q$, wenn a und b bei Division durch q denselben Rest lassen.

Beweis. Es sei $a = \lambda q + r$, $b = \mu q + r'$ mit $0 \leq r, r' < q$. Nun bedeutet $a \equiv b \bmod q$ dasselbe wie $q \mid (r' - r)$. Wegen $|r' - r| < q$ ist dies genau für $r = r'$ der Fall. □

Der nächste Satz ist wegen Satz 1 trivial.

Satz 2. Kongruenz mod$q$ ist eine Äquivalenzrelation auf $\mathbb{Z}$, d.h. es gilt

a) $a \equiv a \bmod q$ (Reflexivität),

b) aus $a \equiv b \bmod q$ folgt $b \equiv a \bmod q$ (Symmetrie),

c) aus $a \equiv b \bmod q$ und $b \equiv c \bmod q$ folgt $a \equiv c \bmod q$ (Transitivität).

Satz 3. Gelten $a \equiv b \bmod q$ und $c \equiv d \bmod q$, so bestehen auch $a + c \equiv b + d \bmod q$ und $ac \equiv bd \bmod q$.

Beweis. Die Differenzen $(a+c) - (b+d) = (a-b) + (c-d)$ und $ac - bd = a(c-d) + (a-b)d$ haben nach Voraussetzung den Teiler q. □

Folgerung 1. Es sei $f(x) \in \mathbb{Z}[x]$, d.h. $f(x) = a_n x^n + \cdots + a_1 x + a_0$ mit $a_n, \ldots, a_1, a_0 \in \mathbb{Z}$. Aus $a \equiv b \bmod q$ folgt dann $f(a) \equiv f(b) \bmod q$.

Definition. Die Äquivalenzklassen $(a)_q := \{m \in \mathbb{Z} : m \equiv a \bmod q\}$ mit $a \in \mathbb{Z}$ heißen Restklassen modulo q.

Folgerung 2. Es gelten die folgenden Aussagen:

a) Die Restklassen mod$q$ definieren eine disjunkte Zerlegung

$$R_q = \{(0)_q\,,\ (1)_q, \ldots\,,\ (q-1)_q\}$$

auf $\mathbb{Z}$, d.h. $\bigcup R_q = \mathbb{Z}$ und aus $(a)_q \cap (b)_q \neq \emptyset$ folgt $(a)_q = (b)_q$.

b) Durch

$$(a)_q + (b)_q = (a+b)_q\,, \quad (a)_q \cdot (b)_q = (a \cdot b)_q$$

sind auf R_q eine Addition und eine Multiplikation definiert. $(R_q\,, +, \cdot)$ ist kommutativer Ring mit Einselement $(1)_q$, der sogenannte Restklassenring modulo q.

Nachweis. Die Behauptungen ergeben sich aus den Sätzen 1, 2 und 3. □

Definition. Jedes System von ganzen Zahlen, das aus jeder Restklasse modulo q genau einen Repräsentanten enthält, heißt ein vollständiges Restsystem modulo q.

Bemerkung 1. Definiert man in dem vollständigen Restsystem

$$\mathbb{Z}/q\mathbb{Z} := \{0, 1, \ldots\,, q-1\}$$

modulo q Summe und Produkt als den jeweiligen Rest der gewöhnlichen Summe bzw. des gewöhnlichen Produkts nach Division durch q, so liegt der Unterschied zwischen $(R_q\,, +, \cdot)$ und $(\mathbb{Z}/q\mathbb{Z}\,, +, \cdot)$ nur in der Schreibweise. Daher ist $(\mathbb{Z}/q\mathbb{Z}\,, +, \cdot)$ ein zu $(R_q\,, +, \cdot)$ isomorpher Ring, den man mit dem Restklassenring modulo q identifiziert.

Beispiel 1. Die Fermatsche Zahl $2^{2^5} + 1 = 2^{32} + 1$ besitzt den Teiler 641 (vgl. Kapitel 1). Der Nachweis verwendet $641 = 5 \cdot 2^7 + 1 = 5^4 + 2^4$. Wir rechnen mit Kongruenzen modulo 641,

$$2^{32} + 1 = 2^4 \cdot 2^{28} + 1 \equiv -5^4 \cdot 2^{28} + 1 = -(5 \cdot 2^7)^4 + 1 \equiv -(-1)^4 + 1 \equiv 0 \bmod 641.$$

Die entsprechende Rechnung in $\mathbb{Z}/641\mathbb{Z}$ lautet

$$2^{32} + 1 = 2^4 \cdot 2^{28} + 1 = -5^4 \cdot 2^{28} + 1 = -(5 \cdot 2^7)^4 + 1 = -(-1)^4 + 1 = 0.$$

Folgerung 3. Ist q nicht Primzahl, so ist $\mathbb{Z}/q\mathbb{Z}$ nicht nullteilerfrei.

Nachweis. Aus der nichttrivialen Zerlegung $q = ab$ mit $1 < a, b < q$ in $\mathbb{Z}$ folgt $ab = 0$ in $\mathbb{Z}/q\mathbb{Z}$ mit $a \neq 0$ und $b \neq 0$. □

Wegen Folgerung 3 ist das Kürzen in Restklassenringen im allgemeinen nicht statthaft. Das untersuchen wir genauer.

Satz 4. Es gelten folgende Aussagen:

a) Genau dann gilt $ac \equiv bc \bmod q$, wenn $a \equiv b \bmod \frac{q}{(q,c)}$ besteht.

b) Für $(q, c) = 1$ sind $ac \equiv bc \bmod q$ und $a \equiv b \bmod q$ gleichwertig.

c) Für $c \in \mathbb{N}$ sind $a \equiv b \bmod q$ und $ac \equiv bc \bmod qc$ gleichwertig.

Beweis. a) Die Teilerbeziehungen $q \mid c(b-a)$ und $\frac{q}{(q,c)} \mid \frac{c}{(q,c)}(b-a)$ sind gleichwertig. Wegen der Teilerfremdheit von $\frac{q}{(q,c)}$ und $\frac{c}{(q,c)}$ folgt die Gleichwertigkeit mit $\frac{q}{(q,c)} \mid (b-a)$, wie behauptet. b) ist der Spezialfall $(q, c) = 1$ von a), und c) ist der Spezialfall $(c, qc) = c$ von a). □

Insbesondere sagt Satz 4 b) aus, daß in Kongruenzen modulo q durch jede zu q teilerfremde Zahl gekürzt werden darf. Damit beweisen wir die Umkehrung von Folgerung 3.

Satz 5. $\mathbb{Z}/q\mathbb{Z}$ ist genau dann Körper, wenn q Primzahl ist.

Beweis. Wegen Folgerung 3 bleibt zu zeigen, daß für Primzahlen q zu jedem $a \in \mathbb{Z}/q\mathbb{Z}$ mit $a \neq 0$ ein $b \in \mathbb{Z}/q\mathbb{Z}$ existiert mit $ab = 1$ in $\mathbb{Z}/q\mathbb{Z}$. Mit $\mathbb{Z}/q\mathbb{Z}$ ist auch

$$a \cdot \mathbb{Z}/q\mathbb{Z} = \{a \cdot 0, a \cdot 1, \ldots, a \cdot (q-1)\}$$

ein vollständiges Restsystem modulo q. Denn die $\nu \cdot a$ mit $\nu = 0, \ldots, q-1$ sind paarweise inkongruent modulo q: Aus $a\nu \equiv a\nu' \bmod q$ folgt $\nu \equiv \nu' \bmod q$ gemäß Folgerung 4 b), also $\nu = \nu'$. Insbesondere ist daher der Rest $1 \bmod q$ in $a \cdot \mathbb{Z}/q\mathbb{Z}$ repräsentiert. Das heißt, es gibt ein $b \in \mathbb{Z}/q\mathbb{Z}$ mit $ab = 1$ in $\mathbb{Z}/q\mathbb{Z}$. □

3.2 Prime Restsysteme

Definition. Es sei $q \in \mathbb{N}$. Jede Restklasse $a \bmod q$ mit $(a, q) = 1$ heißt eine prime Restklasse modulo q. Jedes System von ganzen Zahlen, das aus jeder primen Restklasse modulo q genau einen Repräsentanten enthält, heißt ein reduziertes oder primes Restsystem modulo q.

Beispiel 2. In $\mathbb{Z}/12\mathbb{Z} = \{0, 1, \ldots, 11\}$ ist $\{1, 5, 7, 11\}$ primes Restsystem modulo 12.

Folgerung 4. Es seien $m, n \in \mathbb{N}$ teilerfremd. Dann sind

a) $\{\mu n + \nu m : 1 \leq \mu \leq m,\ 1 \leq \nu \leq n\}$ ein vollständiges Restsystem modulo mn,

b) $\{\mu n + \nu m : 1 \leq \mu \leq m,\ 1 \leq \nu \leq n,\ (\mu, m) = (\nu, n) = 1\}$ ein primes Restsystem modulo mn.

Nachweis. a) Die Zahlen $\mu n + \nu m$ mit $1 \leq \mu \leq m$ und $1 \leq \nu \leq n$ sind paarweise inkongruent modulo mn. Denn aus $\mu n + \nu m \equiv \mu' n + \nu' m \bmod mn$ kommt $(\mu - \mu')n \equiv (\nu' - \nu)m \bmod mn$, also $(\mu - \mu')n \equiv 0 \bmod m$ und $(\nu' - \nu)m \equiv 0 \bmod n$. Wegen $(m, n) = 1$ liefert Satz 4 b) die Kongruenzen $\mu \equiv \mu' \bmod m$ und $\nu \equiv \nu' \bmod n$, die infolge $|\mu - \mu'| < m$ und $|\nu - \nu'| < n$ nur für $\mu = \mu'$ und $\nu = \nu'$ möglich sind.

b) Damit $\mu n + \nu m$ eine prime Restklasse modulo mn repräsentiert, ist ersichtlich die Bedingung $(\mu, m) = (\nu, n) = 1$ notwendig. Sie ist auch hinreichend. Gäbe es nämlich eine Primzahl p mit $p \mid mn$ und $p \mid (\nu m + \mu n)$, also etwa $p \mid n$, so käme $p \mid \nu m$, was wegen $(\nu, n) = 1$ auf $p \mid m$ führt. Das widerspricht $(m, n) = 1$. Ein Rückgriff auf a) erledigt den Nachweis von b). □

Definition. Für $q \in \mathbb{N}$ bezeichnet

$$G(q) = \{a \in \mathbb{N} : 1 \le a \le q\,,\ (a, q) = 1\}$$

ein primes Restsystem modulo q und

$$\varphi(q) = \sum_{a \in G(q)} 1$$

seine Elementeanzahl. Die Funktion $\varphi : \mathbb{N} \to \mathbb{N}$ heißt Eulerfunktion.

Satz 6. Es ist $(G(q), \cdot\,) \subseteq (\mathbb{Z}/q\mathbb{Z}\,, \cdot\,)$ eine abelsche Gruppe, genannt prime Restklassengruppe modulo q. Ihre Gruppenordnung $\varphi(q)$ ist eine multiplikative Funktion, d.h. es gilt $\varphi(1) = 1$ und $\varphi(mn) = \varphi(m)\,\varphi(n)$ für alle teilerfremden $m, n \in \mathbb{N}$.

Beweis. Das Produkt primer Reste mod q ist wieder primer Rest mod q. Daher führt die Restklassenmultiplikation aus $G(q)$ nicht heraus. Es gilt $1 \in G(q)$, und für $a \in G(q)$ ist mit $G(q)$ auch $a\,G(q)$ ein primes Restsystem modulo q. Da in $a\,G(q)$ speziell 1 repräsentiert ist, existiert zu $a \in G(q)$ stets ein $b \in G(q)$ mit $ab \equiv 1 \bmod q$. Das heißt, jedes $a \in G(q)$ ist in $G(q)$ invertierbar. Die Multiplikativität der Eulerfunktion kommt unmittelbar aus Folgerung 4 b). □

Folgerung 5. Es gilt

$$\varphi(q) = q \prod_{p \mid q} \Big(1 - \frac{1}{p}\Big),$$

wobei das Produkt über alle Primteiler p von q erstreckt ist.

Nachweis. Für $p \in \mathbb{P}$ und $\nu \in \mathbb{N}$ ist $\varphi(p^\nu)$ die Anzahl der zu p^ν teilerfremden Zahlen aus $G(p^\nu)$, also die Anzahl der nicht durch p teilbaren natürlichen Zahlen $a \le p^\nu$. Das heißt

$$\varphi(p^\nu) = \sum_{\substack{1 \le a \le p^\nu \\ p \nmid a}} 1 = \sum_{1 \le a \le p^\nu} 1 - \sum_{\substack{1 \le a \le p^\nu \\ p \mid a}} 1 = p^\nu - p^{\nu-1} = p^\nu \Big(1 - \frac{1}{p}\Big).$$

Die allgemeine Behauptung kommt nun aus Satz 6. □

Beispiel 3. $\varphi(12) = \varphi(3)\,\varphi(4) = (3-1)(4-2) = 4$.

Satz 7. Es gilt $\sum_{d \mid q} \varphi(d) = q$, wobei die Summation über alle natürlichen Teiler d von q läuft.

Beweis. Wir betrachten die Mengen

$$A_d = \{a \in \mathbb{N} : 1 \le a \le q\,,\ (a, q) = d\}$$

und stellen die folgenden Eigenschaften fest:

a) Die A_d mit $d \mid q$ bilden eine disjunkte Zerlegung von $\{1, \dots, q\}$.

b) $A_d = \{da' : 1 \le a' \le \frac{q}{d},\ (a', \frac{q}{d}) = 1\}$, also $|A_d| = \sum_{a \in A_d} 1 = \varphi(\frac{q}{d})$.

Aus a) und b) folgt durch Übergang zu den Elementeanzahlen

$$q = \sum_{d|q} |A_d| = \sum_{d|q} \varphi(\frac{q}{d}) = \sum_{d|q} \varphi(d),$$

wobei zuletzt die Teiler $\frac{q}{d}$ durch die komplementären Teiler d von q ersetzt wurden. □

Satz 8. (Euler) Für $(a, q) = 1$ gilt $a^{\varphi(q)} \equiv 1 \bmod q$.

Beweis. Da $G(q) = \{a_1, \dots, a_{\varphi(q)}\}$ gemäß Satz 6 eine abelsche Gruppe der Ordnung $\varphi(q)$ ist, besteht $a\,G(q) = G(q)$ für jedes $a \in G(q)$. Es folgt

$$(aa_1) \cdots (aa_{\varphi(q)}) \equiv a_1 \cdots a_{\varphi(q)} \bmod q.$$

Nach Satz 4 b) darf hierin durch $a_1 \cdots a_{\varphi(q)}$ gekürzt werden. □

Folgerung 6. Als Spezialfall $q = p \in \mathbb{P}$ folgt mit $\varphi(p) = p - 1$ aus Satz 8 der sogenannte „kleine Fermatsche Satz“: Für Primzahlen p und $a \in \mathbb{Z}$ mit $p \nmid a$ gilt $a^{p-1} \equiv 1 \bmod p$. Eine äquivalente Version lautet $a^p \equiv a \bmod p$ für alle $p \in \mathbb{P}$ und $a \in \mathbb{Z}$.

Eine Anwendung von Folgerung 6 ist die

Folgerung 7. Es sei $1 \neq a \in \mathbb{N}$. Dann hat jeder ungerade Primteiler p von $a^{2^r} + 1$ die Gestalt $p = k \cdot 2^{r+1} + 1$ mit $k \in \mathbb{N}$. (Zum Beispiel gilt $10 \cdot 2^6 + 1 = 641 \mid 2^{32} + 1$)

Nachweis. Es sei $h \in \mathbb{N}$ minimal gewählt mit $a^h \equiv 1 \bmod p$. Dann heißt h die Ordnung von $a \in G(p)$. Wir behaupten

(i) $h \mid (p-1)$, (ii) $h = 2^{r+1}$.

Hieraus kommt offenbar die Behauptung von Folgerung 7. Zum Beweis von (i) dividieren wir $p - 1$ mit Rest durch h, also $p - 1 = \lambda h + \varrho$, $0 \le \varrho < h$. Aus Folgerung 6 entsteht $1 \equiv a^{p-1} = (a^h)^\lambda \cdot a^\varrho \equiv a^\varrho \bmod p$. Wegen der Minimalität von h folgt $\varrho = 0$, also $h \mid p - 1$. Zum Beweis von (ii) dividieren wir 2^{r+1} mit Rest durch h, also $2^{r+1} = \mu h + \sigma$, $0 \le \sigma < h$. Wie in (i) folgt $\sigma = 0$, also $h \mid 2^{r+1}$. Wäre schon $h \mid 2^r$, also $2^r = \mu h$, so wäre schon $a^{2^r} \equiv (a^h)^\mu \equiv 1 \bmod p$ im Widerspruch zu $a^{2^r} \equiv -1 \bmod p$. Also ist $h = 2^{r+1}$. □

Wir haben einen algebraischen Sachverhalt entdeckt: Es sei G eine Gruppe (mit multiplikativ geschriebener Verknüpfung), und es sei $h \in \mathbb{N}$ die Ordnung von $g \in G$. Ist $g^m = e$ (Einselement) für ein $m \in \mathbb{N}$, so gilt $h \mid m$.

Der folgende Satz geht auf Wilson (1741 - 1793) zurück.

Satz 9. (Wilsonsche Kongruenz) Es sei $1 \neq n \in \mathbb{N}$. Genau für Primzahlen n gilt

$$(n-1)! \equiv -1 \bmod n.$$

Beweis. a) Ist $n \notin \mathbb{P}$, so existiert ein Teiler d von n mit $1 < d < n$, und es folgt $(n-1)! \equiv 0 \not\equiv -1 \bmod d$, erst recht $(n-1)! \not\equiv -1 \bmod n$.
b) Für $p = 2$ gilt offenbar $(p-1)! = 1 \equiv -1 \bmod p$. Für ungerades $n = p \in \mathbb{P}$ betrachten wir das Produkt aller Elemente der primen Restklassengruppe $G(p) = \{1, 2, \ldots, p-1\}$. Zu jedem $a \in G(p)$ liegt auch das multiplikativ Inverse in $G(p)$. Dabei gilt $a \cdot a \equiv 1 \bmod p$ genau für $(a-1)(a+1) \equiv 0 \bmod p$, also genau für $a = 1$ und $a = p-1$ ($a \in G(p)$). Bei geeigneter Zusammenfassung der Faktoren $2, \ldots, p-2$ zu Paaren modulo p inverser Zahlen erhalten wir

$$(p-1)! = 1 \cdot \big(2 \cdot 3 \cdots (p-3) \cdot (p-2)\big) \cdot (p-1) \equiv -1 \bmod p\,,$$

wie behauptet. □

Bemerkung 3. Satz 9 liefert ein bekanntes Primzahlkriterium, dessen praktischer Nutzen wegen des Wachstums der Fakultät begrenzt ist.

Kapitel 4

Polynomkongruenzen

In diesem Kapitel werden lineare Kongruenzen und Kongruenzsysteme sowie Polynomkongruenzen behandelt.

4.1 Lineare Kongruenzen

Satz 1. Es seien $a, b \in \mathbb{Z}$, $q \in \mathbb{N}$. Genau dann ist die Kongruenz $ax \equiv b \bmod q$ lösbar, wenn $(a,q) \mid b$ gilt. In diesem Fall gibt es genau eine Restklasse $\bmod \frac{q}{(a,q)}$, welche die Kongruenz löst, also genau (a,q) Lösungen $\bmod q$.

Beweis. Ist $\xi \in \mathbb{Z}$ Lösung von $ax \equiv b \bmod q$, so gilt $q \mid (a\xi - b)$, also $(a,q) \mid b$.

Umgekehrt gelte $(a,q) \mid b$. Die Lösbarkeit von $ax \equiv b \bmod q$ ist äquivalent zur Lösbarkeit der diophantischen Gleichung

$$a'x + q'y = b' \tag{1}$$

mit $a' = \frac{a}{(a,q)}$, $b' = \frac{b}{(a,q)}$, $q' = \frac{q}{(a,q)}$. Gemäß Kapitel 2, Satz 5, existiert genau eine Restklasse $x_0 \bmod q'$, welche (1) löst. Sie zerfällt in genau (a,q) Restklassen $x_0 + \lambda q' \bmod q$ mit $\lambda = 0, 1, \ldots, (a,q) - 1$. Das war behauptet. □

Beispiel 1. Die Kongruenz $12x \equiv 9 \bmod 27$ ist wegen $(12, 27) = 3 \mid 9$ nach Satz 1 lösbar. Nach den Kürzungsregeln ist sie äquivalent zu $4x \equiv 3 \bmod 9$ oder auch $4x \equiv 12 \bmod 9$, also zu $x \equiv 3 \bmod 9$. Die gesuchten Restklassen $\bmod 27$ sind demnach $3, 12, 21 \bmod 27$. Bei größeren Moduln führt stets der Euklidische Algorithmus zum Ziel.

Bemerkung 1. Für $q_1, \ldots, q_r \in \mathbb{N}$ besteht $a \equiv b \bmod q_\varrho$ für $\varrho = 1, \ldots, r$ genau dann, wenn $a \equiv b \bmod [q_1, \ldots, q_r]$ gilt. Hat speziell $q \in \mathbb{N}$ die kanonische Zerlegung $q = p_1^{\nu_1} \cdots p_r^{\nu_r}$, so gilt $a \equiv b \bmod q$ genau für $a \equiv b \bmod p_\varrho^{\nu_\varrho}$ mit $\varrho = 1, \ldots, r$.

Nachweis. Es wird Folgerung 6 b), c) aus Kapitel 2 angewandt. □

Satz 2. Es sei $q \in \mathbb{N}$, $a_\varrho, b \in \mathbb{Z}$ für $\varrho = 1, \dots, r$ und $d = (a_1, \dots, a_r, q)$. Genau dann ist die Kongruenz

$$a_1 x_1 + \cdots + a_r x_r \equiv b \bmod q$$

lösbar, wenn $d \mid b$ gilt. In diesem Fall gibt es genau dq^{r-1} r-tupel $(\xi_1, \dots, \xi_r)$ von Restklassen $\xi_\varrho \bmod q$, welche die Kongruenz lösen.

Beweis. Für $r = 1$ erledigt Satz 1 die Behauptung. Die Bedingung $d \mid b$ ist trivialerweise notwendig. Wir zeigen induktiv, daß sie hinreichend ist. Dazu nehmen wir die Richtigkeit des Satzes für $r-1$ statt r an und setzen $d' = (a_1, \dots, a_{r-1}, q)$. Dann ist also $(d', a_r) = d$. Die Kongruenz

$$a_r x_r \equiv b \bmod d'$$

hat nach Satz 1 genau $(a_r, d') = d$ Lösungen $\bmod d'$, also genau $d \cdot \frac{q}{d'}$ Lösungen $\xi_r \bmod q$. Zu jeder derartigen Lösung ξ_r setzen wir

$$b' = \frac{(b - a_r \xi_r)}{d'}.$$

Laut Induktionsannahme hat die Kongruenz $a_1 x_1 + \cdots a_{r-1} x_{r-1} \equiv b' d' \bmod q$ genau $d' q^{r-2}$ Lösungen $(\xi_1, \dots, \xi_{r-1}) \bmod q$. Also ist die Anzahl aller Lösungen $(\xi_1, \dots, \xi_r) \bmod q$ der Kongruenz $a_1 x_1 + \cdots + a_r x_r = b \bmod q$ gleich $d \frac{q}{d'} \cdot d' q^{r-2} = dq^{r-1}$. Das war behauptet. □

Beispiel 2. Die Kongruenz $2x + 6y \equiv 4 \bmod 8$ ist lösbar wegen $(2, 4, 8) = 2 \mid 4$. Sie ist äquivalent zu $x + 3y \equiv 2 \bmod 4$. Es gibt genau 4 Paare von Restklassen $\bmod 4$, die diese Kongruenz lösen. Wegen $(1, 4) = 1$ sehen wir alle möglichen Restklassen $y \equiv 0, 1, 2, 3 \bmod 4$ nach. Es folgt jeweils $x \equiv 2 + y \bmod 4$, also $x \equiv 2, 3, 0, 1 \bmod 4$ resp. Damit haben wir alle vier Lösungspaare $(2; 0), (3; 1), (0; 2), (1; 3) \bmod 4$ (das ergibt 16 Lösungspaare $\bmod 8$).

Satz 3. Für $\varrho = 1, \dots, r$ seien $a_\varrho, b_\varrho \in \mathbb{Z}$, $q_\varrho \in \mathbb{N}$ mit $(a_\varrho, q_\varrho) = 1$, und die q_ϱ seien paarweise teilerfremd. Dann ist das lineare Kongruenzsystem

$$(\mathsf{S_r}) \qquad a_\varrho x \equiv b_\varrho \bmod q_\varrho \quad (\varrho = 1, \dots, r)$$

lösbar, und zwar durch genau eine Restklasse $\bmod q_1 \cdots q_r$.

Beweis. Wir führen den Beweis in zwei Schritten.

a) Ist $\xi \in \mathbb{Z}$ eine Lösung von $(\mathsf{S_r})$, so löst die ganze Restklasse $\xi \bmod q_1 \cdots q_r$ das System $(\mathsf{S_r})$, und weitere Lösungen existieren nicht.

Denn es gilt $a_\varrho(\xi + t q_1 \cdots q_r) \equiv b_\varrho \bmod q_1 \cdots q_r$ für jedes $t \in \mathbb{Z}$. Sind ξ, ξ' Lösungen von $(\mathsf{S_r})$, so folgt $a_\varrho(\xi - \xi') \equiv 0 \bmod q_\varrho$, wegen $(a_\varrho, q_\varrho) = 1$ also $\xi \equiv \xi' \bmod q_\varrho$ für $\varrho = 1, \dots, r$. Das heißt, es gilt $\xi \equiv \xi' \bmod q_1 \cdots q_r$.

b) $(\mathsf{S_r})$ hat eine Lösung.

Für $r = 1$ liefert Satz 1 die Behauptung. Es sei nun ξ eine Lösung von $(\mathsf{S_{r-1}})$. Zu zeigen ist, daß dann auch $(\mathsf{S_r})$ lösbar ist, also das System

$$(2) \qquad \begin{cases} x & \equiv & \xi \bmod q_1 \cdots q_{r-1} \\ a_r x & \equiv & b_r \bmod q_r. \end{cases}$$

Nun ist (2) äquivalent zu $a_r(\xi + t \cdot q_1 \cdots q_{r-1}) \equiv b_r \bmod q_r$ also zu

$$a_r q_1 \cdots q_{r-1} \cdot t + q_r \cdot s = b_r - a_r \xi \,. \tag{3}$$

Nach Kapitel 2, Satz 5, lautet die notwendige und hinreichende Lösbarkeitsbedingung von (3)

$$(a_r q_1 \cdots q_{r-1}, q_r) \mid b_r - a_r \xi \,.$$

Nach Voraussetzung steht links 1. Daraus folgt die Behauptung. □

Bemerkung 2. Ist die Bedingung $(a_\varrho, q_\varrho) = 1$ nicht von vornherein erfüllt, ist $(a_\varrho, q_\varrho) \mid b_\varrho$ die notwendige und hinreichende Lösbarkeitsbedingung für die ϱ-te Kongruenz. Diese läßt sich dann geeignet reduzieren. Gilt $(a_\varrho, q_\varrho) \nmid b_\varrho$, so ist die ϱ-te Kongruenz bereits unlösbar; erst recht $(\mathsf{S_r})$.

Die paarweise Teilerfremdheit der q_ϱ in Satz 12 kann ersetzt werden durch die Bedingung

$$(q_\varrho, q_\sigma) \mid (a_\varrho b_\sigma - a_\sigma b_\varrho) \qquad (1 \le \varrho < \sigma \le r).$$

Sie ist hinreichend und notwendig für die Lösbarkeit des Systems $(\mathsf{S_r})$. Es existiert dann genau eine Lösungsrestklasse $\bmod [q_1, \ldots, q_r]$.

Folgerung 1. Ein Spezialfall von Satz 3 ist der sogenannte Chinesische Restsatz:
Sind $q_1, \ldots, q_r \in \mathbb{N}$ paarweise teilerfremd und $b_1, \ldots, b_r \in \mathbb{Z}$, so besitzt das Kongruenzsystem

$$x \equiv b_\varrho \bmod q_\varrho \qquad (\varrho = 1, \ldots, r)$$

genau eine Lösung $\bmod q_1 \cdots q_r$.

Beispiel 3. Das Kongruenzsystem $2x \equiv 3 \bmod 5$, $3x \equiv 2 \bmod 10$ ist äquivalent zu $2x \equiv 3 \bmod 5$, $3x \equiv 2 \bmod 5$, $x \equiv 0 \bmod 2$, also zu $2x \equiv 3 \bmod 5$, $x \equiv 0 \bmod 2$. Mit $x = 2y$ geht dies über in die äquivalente Kongruenz $4y \equiv 3 \bmod 5$ mit der eindeutigen Lösung $y \equiv 2 \bmod 5$, also $x \equiv 4 \bmod 10$.

4.2 Nichtlineare Kongruenzen

Es sei $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ ein Polynom mit ganzen Koeffizienten. Wir behandeln Polynomkongruenzen $f(x) \equiv 0 \bmod q$. Aus Kapitel 3, Folgerung 1, ist bekannt, daß mit jeder Lösung $\xi \in \mathbb{Z}$ alle Zahlen $\equiv \xi \bmod q$ Lösungen sind.

Definition. Unter der Lösungsanzahl $\varrho_f(q)$ der Polynomkongruenz $f(x) \equiv 0 \bmod q$ versteht man die Anzahl der Restklassen $\bmod q$, die die Kongruenz lösen.

Satz 4. Es sei $q = q_1 \cdots q_k$ mit paarweise teilerfremden $q_\kappa \in \mathbb{N}$. Dann ist die Polynomkongruenz $f(x) \equiv 0 \bmod q$ äquivalent zum System der Polynomkongruenzen $f(x) \equiv 0 \bmod q_\kappa$ mit $\kappa = 1, \ldots, k$. Die Funktion $\varrho_f : \mathbb{N} \to \mathbb{N}_0$ ist multiplikativ.

Beweis. Die erste Aussage ist trivial (vgl. Bemerkung 1). Zum Nachweis der Multiplikativität von ϱ_f seien $m, n \in \mathbb{N}$ teilerfremd und $\xi_1, \ldots, \xi_s \bmod m$ alle Lösungen von $f(x) \equiv 0 \bmod m$, $\eta_1, \ldots, \eta_t \bmod n$ alle Lösungen von $f(x) \equiv 0 \bmod n$.

Für jedes Paar $(\xi;\eta)$ dieser Lösungen ist das lineare Kongruenzsystem

$$x \equiv \xi \bmod m\,, \quad x \equiv \eta \bmod n$$

nach dem Chinesischen Restsatz eindeutig modulo mn lösbar. Für verschiedene Paare $(\xi;\eta)$ sind die Lösungen inkongruent modulo mn. Also gilt $\varrho_f(mn) = \varrho_f(m)\,\varrho_f(n)$. □

Wegen Satz 4 brauchen nur noch Polynomkongruenzen mit Primzahlpotenzmoduln untersucht zu werden. Tatsächlich genügt es, sich mit Primzahlmoduln zu beschäftigen. Wir bemerken dazu, daß jede Lösung ξ von $f(x) \equiv 0 \bmod p^{\nu+1}$ auch Lösung von $f(x) \equiv 0 \bmod p^{\nu}$ ist. Ist also ξ eine Lösung von $f(x) \equiv 0 \bmod p^{\nu}$, so ist jede zu ξ gehörige Lösung von $f(x) \equiv 0 \bmod p^{\nu+1}$ in der Restklasse $\xi \bmod p^{\nu}$ zu finden. Dies führt auf die Kongruenz

$$f(\xi + tp^{\nu}) \equiv 0 \bmod p^{\nu+1}$$

für t. Nun ist

$$\begin{aligned} f(\xi + tp^{\nu}) &= a_n(\xi + tp^{\nu})^n + \cdots + a_1(\xi + tp^{\nu}) + a_0 \\ &\equiv f(\xi) + t\,p^{\nu} f'(\xi) \bmod p^{\nu+1}. \end{aligned}$$

Wegen $p^{\nu} \mid f(\xi)$ bleibt zu lösen

$$f'(\xi)\,t \equiv -\frac{f(\xi)}{p^{\nu}} \bmod p\,.$$

Dies ist eine lineare Kongruenz mit der Lösungsanzahl

$$\begin{aligned} &1\,, \quad \text{falls } p \nmid f'(\xi) \\ &0\,, \quad \text{falls } p \mid f'(\xi) \text{ und } p \nmid \frac{f(\xi)}{p^{\nu}} \\ &p\,, \quad \text{falls } p \mid f'(\xi) \text{ und } p \mid \frac{f(\xi)}{p^{\nu}}\,. \end{aligned}$$

Damit ist die Strategie klar, wie man von Lösungen von $f(x) \equiv 0 \bmod p^{\nu}$ zu denen von $f(x) \equiv 0 \bmod p^{\nu+1}$ aufsteigt. Es bleiben daher noch Polynomkongruenzen mit Primzahlmoduln zu lösen. Dafür gibt es kein allgemeines Verfahren.

Beispiel 4. Die Polynomkongruenz $x^2 + 3x + 2 \equiv 0 \bmod 72$ ist zu lösen.

Wegen $72 = 2^3 \cdot 3^2$ bestimmen wir die Lösung $\bmod 2^3$ und $\bmod 3^2$ einzeln gemäß Satz 4.

a) Lösungen $\bmod 2$: $x^2 + 3x + 2 \equiv 0 \bmod 2 \iff x \equiv 0 \bmod 2$ oder $x \equiv 1 \bmod 2$

Lösungen $\bmod 4$: $x^2 + 3x + 2 \equiv 0 \bmod 4 \iff$

$x = 2t$: $4t^2 + 6t + 2 \equiv 0 \bmod 4 \iff t \equiv 1 \bmod 2 \iff x \equiv 2 \bmod 4$
$x = 2t + 1$: $4t^2 + 10t + 6 \equiv 0 \bmod 4 \iff t \equiv 1 \bmod 2 \iff x \equiv 3 \bmod 4$

Lösungen $\bmod 8$: $x^2 + 3x + 2 \equiv 0 \bmod 4 \iff$

$x = 4t + 2$: $16t^2 + 28t + 12 \equiv 0 \bmod 8 \iff t \equiv 1 \bmod 2 \iff x \equiv 6 \bmod 8$
$x = 4t + 3$: $16t^2 + 36t + 20 \equiv 0 \bmod 8 \iff t \equiv 1 \bmod 2 \iff x \equiv 7 \bmod 8$

Zwischenergebnis: $x^2 + 3x + 2 \equiv 0 \bmod 8$ hat genau die Lösungen $x \equiv 6 \bmod 8$ und $x \equiv 7 \bmod 8$.

b) Lösungen mod 3: $x^2+3x+2 \equiv 0 \bmod 3 \iff x \equiv 1 \bmod 3$ oder $x \equiv 2 \bmod 3$

Lösungen mod 9: $x^2+3x+2 \equiv 0 \bmod 9 \iff$

$x = 3t+1$: $9t^2+15t+6 \equiv 0 \bmod 9 \iff t \equiv 2 \bmod 3 \iff x \equiv 7 \bmod 9$
$x = 3t+2$: $9t^2+21t+12 \equiv 0 \bmod 9 \iff t \equiv 2 \bmod 3 \iff x \equiv 8 \bmod 9$

Zwischenergebnis: $x^2+3x+2 \equiv 0 \bmod 9$ hat genau die Lösungen $x \equiv 7 \bmod 9$ und $x \equiv 8 \bmod 9$.

c) Alle Lösungen von $x^2+3x+2 \equiv 0 \bmod 72$ entstehen durch Kombination aller Lösungen mod 8 mit allen Lösungen mod 9. Dies liefert folgende Kongruenzsysteme, die nach dem Chinesischen Restsatz alle eindeutig lösbar mod 72 sind:

$$\left.\begin{array}{rcl} x & \equiv & 6 \bmod 8 \\ x & \equiv & 7 \bmod 9 \end{array}\right\} \iff x \equiv -2 \bmod 72\,;$$

$$\left.\begin{array}{rcl} x & \equiv & 6 \bmod 8 \\ x & \equiv & 8 \bmod 9 \end{array}\right\} \iff x \equiv -10 \bmod 72\,;$$

$$\left.\begin{array}{rcl} x & \equiv & 7 \bmod 8 \\ x & \equiv & 7 \bmod 9 \end{array}\right\} \iff x \equiv 7 \bmod 72\,;$$

$$\left.\begin{array}{rcl} x & \equiv & 7 \bmod 8 \\ x & \equiv & 8 \bmod 9 \end{array}\right\} \iff x \equiv -1 \bmod 72\,.$$

Also sind alle Lösungen von $x^2+3x+2 \equiv 0 \bmod 72$ gegeben durch $x \equiv -1, -2, 7, -10 \bmod 72$.

d) Man hätte sich die ganze Arbeit sparen können, wenn man die Zerlegung $x^2+3x+2 = (x+1)(x+2)$ verwendet hätte. In $\mathbb{Z}/72\mathbb{Z}$ ist $(x+1)(x+2) = 0$ äquivalent dazu, daß ein Faktor verschwindet, also $x = -1$ oder $x = -2$, oder beide Faktoren sind komplementäre Nullteiler, also $x = 7$ oder $x = -10$.

Bemerkung 3. Es sei $q \in \mathbb{N}$, $f(x) \in \mathbb{Z}[x]$, $\deg f(x) \geq 0$, und $a \in \mathbb{Z}$ eine Lösung von $f(x) \equiv 0 \bmod q$. Dann gibt es ein Polynom $g(x) \in \mathbb{Z}[x]$ mit $\deg g(x) = -1 + \deg f(x)$ und $f(x) \equiv (x-a)g(x) \bmod q$ für alle $x \in \mathbb{Z}$. Es ist nämlich

$$f(x) - f(a) = a_n(x^n - a^n) + \ldots + a_1(x-a) = (x-a)g(x),$$

so daß die Differenz $f(x) - (x-a)g(x) = f(a)$ durch q teilbar ist. Etwa gilt in Beispiel 4: $x^2+3x+2 = (x+1)(x+2) = (x-7)(x+10)$ in $\mathbb{Z}/72\mathbb{Z}$.

Satz 5. (Lagrange, 1736 - 1813) Es sei $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$, $p \in \mathbb{P}$ und $p \nmid a_n$. Dann hat die Kongruenz $f(x) \equiv 0 \bmod p$ höchstens n Lösungen.

Beweis. Für $n = 0$ ist die Aussage trivial, für $n = 1$ folgt sie aus Satz 1. Wir nehmen an, die Behauptung trifft für $n-1$ statt n zu. Es sei $a \in \mathbb{Z}$ eine Lösung von $f(x) \equiv 0 \bmod p$. Mit geeignetem $g(x) = a_n x^{n-1} + \cdots \in \mathbb{Z}[x]$ gilt nach obiger Bemerkung $f(x) \equiv (x-a)g(x) \bmod p$ für alle $x \in \mathbb{Z}$. Ist nun $\xi \in \mathbb{Z}$ eine Lösung von $f(x) \equiv 0 \bmod p$, so gilt $f(\xi) \equiv (\xi - a)g(\xi) \bmod p$, also $(\xi - a) \equiv 0 \bmod p$ oder $g(\xi) \equiv 0 \bmod p$ wegen $p \in \mathbb{P}$. Die Behauptung folgt aus der Induktionsannahme. □

Bemerkung 4. Wie Beispiel 4 zeigt, ist für Nichtprimzahlmoduln die Aussage von Satz 5 falsch.

Folgerung 2. Es sei $f(x) \in \mathbb{Z}[x]$, $n = \deg f(X) \in \mathbb{N}_0$, $p \in \mathbb{P}$, und die Polynomkongruenz $f(x) \equiv 0 \bmod p$ habe mehr als n Lösungen. Dann sind alle Koeffizienten des Polynoms $f(x)$ durch p teilbar. Das heißt, in $(\mathbb{Z}/p\mathbb{Z})[x]$ ist $f(x)$ das Nullpolynom.

Nachweis. Nach Voraussetzung hat $f(x) = a_n x^n + \cdots + a_1 x + a_0$ mehr als n Nullstellen in $\mathbb{Z}/p\mathbb{Z}$. Satz 5 liefert $p \mid a_n$ und $a_n x^n \equiv 0 \bmod p$ für alle x. Also hat das Polynom $a_{n-1}x^{n-1} + \cdots + a_0$ mehr als n Nullstellen, es folgt $p \mid a_{n-1}$, usw. □

Bemerkung 5. Folgerung 2 ermöglicht einen neuen Beweis der Wilsonschen Kongruenz $(p-1)! \equiv -1 \bmod p$ für $p \in \mathbb{P}$

Nach dem kleinen Fermatschen Satz gilt $a^{p-1} \equiv 1 \bmod p$ für alle $a \in \mathbb{Z}$ mit $p \nmid a$. Mit $f(x) = x^{p-1} - 1$ hat die Kongruenz $f(x) \equiv 0 \bmod p$ die $p-1$ Lösungen $1, 2, \ldots, p-1 \bmod p$. Dasselbe trifft auf $g(x) = (x-1)(x-2)\cdots(x-(p-1))$ zu. Das Differenzpolynom $h(x) = f(x) - g(x)$ $h(x) \equiv 0 \bmod p$ hat einen Grad $< p-1$, aber mindestens $p-1$ Nullstellen in $\mathbb{Z}/p\mathbb{Z}$. Aus Folgerung 2 kommt speziell $p \mid (f(0) - g(0))$, also $(p-1)! \equiv (-1)^p \bmod p$. Beachtet man noch $(-1)^p \equiv -1 \bmod p$ für alle $p \in \mathbb{P}$, so folgt $(p-1)! \equiv -1 \bmod p$.

Kapitel 5

Quadratische Kongruenzen

Das Hauptergebnis dieses Kapitels ist das von Gauß 1796 (im Alter von 19 Jahren) bewiesene quadratische Reziprozitätsgesetz.

5.1 Das Legendre-Symbol

Die allgemeine quadratische Kongruenz

$$Ax^2 + Bx + C \equiv 0 \bmod q$$

mit $A, B, C \in \mathbb{Z}$, $q \in \mathbb{N}$ ist nach Kapitel 4, Satz 4, äquivalent zu dem System der quadratischen Kongruenzen

$$Ax^2 + Bx + C \equiv 0 \bmod p^\nu \qquad (p^\nu \| q).$$

Dabei steht $p^\nu \| q$ für $p^\nu \mid q$ und $p^{\nu+1} \nmid q$. Jede Lösung $\bmod p^\nu$ ist auch Lösung $\bmod p$, und in Kapitel 4 wurde gezeigt, wie man von Lösungen $\bmod p$ zu solchen $\bmod p^2$, $p^3, \ldots$ aufsteigt (wenn möglich). Daher genügt es, quadratische Kongruenzen

$$Ax^2 + Bx + C \equiv 0 \bmod p$$

mit Primzahlmoduln p zu untersuchen. Dabei darf $p \neq 2$ vorausgesetzt werden, da die Lösbarkeit für $p = 2$ durch triviales Probieren zu testen ist. Ferner darf $p \nmid A$ angenommen werden, da die Kongruenz sonst linear ist. Nach dem kleinen Fermatschen Satz ist $A^{p-1} \equiv 1 \bmod p$, und bei Durchmultiplikation der quadratischen Kongrenz mit A^{p-2} sieht man, daß $A = 1$ vorausgesetzt werden darf. Wegen $B \equiv B + p \mod p$ für jede ungerade Primzahl p darf B als gerade angenommen werden. Mit gewissen Koeffizienten $b, c \in \mathbb{Z}$ hat man also die quadratische Kongruenz $x^2 + 2bx + c \equiv 0 \bmod p$ zu untersuchen, also $(x + b)^2 \equiv b^2 - c \bmod p$. Schreibt man darin a statt $b^2 - c$ und x statt $x + b$, so bleibt

$$x^2 \equiv a \bmod p \tag{1}$$

zu behandeln. Für $p \mid a$ hat man als triviale Lösung genau die Restklasse $0 \bmod p$. Ist die Kongruenz für $p \nmid a$ lösbar, so gibt es genau zwei inkongruente Lösungen $\bmod p$. Wir fassen zusammen:

Bemerkung 1. Das Problem der Lösbarkeit quadratischer Kongruenzen ist reduziert auf die Lösbarkeit von (1) mit $2 \neq p \in \mathbb{P}$ und $a \in \mathbb{Z}$. Im Fall $p \mid a$ gibt es genau eine Lösung, nämlich $0 \mod p$. Im Fall $p \nmid a$ besitzt die Kongruenz (1) entweder keine oder genau zwei $\bmod p$ inkongruente Lösungen.

Definition. Es sei $2 \neq p \in \mathbb{P}$, $p \nmid a \in \mathbb{Z}$. Ist (1) lösbar, so heißt a quadratischer Rest (R) modulo p, andernfalls quadratischer Nichtrest (N) modulo p. Für $2 \neq p \in \mathbb{P}$ und $a \in \mathbb{Z}$ ist das Legendre-Symbol $\left(\frac{a}{p}\right)$ (gelesen: a nach p) erklärt durch

$$\left(\frac{a}{p}\right) = \begin{cases} 0\,, & \text{falls } p \mid a \\ 1\,, & \text{falls } a \text{ quadratischer Rest } \bmod p \\ -1\,, & \text{falls } a \text{ quadratischer Nichtrest } \bmod p\,. \end{cases}$$

Das Problem der Lösbarkeit von (1) ist also äquivalent zur Bestimmung des Legendre-Symbols $\left(\frac{a}{p}\right)$. Wir notieren die triviale

Folgerung 1. Es sei $2 \neq p \in \mathbb{P}$.

a) Jede Quadratzahl m^2 mit $p \nmid m \in \mathbb{Z}$ ist quadratischer Rest modulo p:
$\left(\frac{m^2}{p}\right) = 1$ für $p \nmid m \in \mathbb{Z}$.

b) Das Legendre-Symbol nach p ist eine p-periodische Funktion:
$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ für $a \equiv b \mod p$.

Beispiel 1. $\left(\frac{1}{3}\right) = 1$, $\left(\frac{2}{3}\right) = -1$; $\left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = 1$, $\left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1$.

Satz 1. Für $2 \neq p \in \mathbb{P}$ gelten die folgenden Aussagen.

a) Es gibt ebensoviele quadratische Reste wie Nichtreste modulo p.

b) Die sämtlichen quadratischen Reste modulo p werden repräsentiert durch die Zahlen m^2 mit $m \in \mathbb{N}$ mit $1 \leq m \leq \frac{p-1}{2}$.

Beweis. a) Wegen Folgerung 1 a) sind die Zahlen m^2 mit $1 \leq m \leq \frac{p-1}{2}$ quadratische Reste modulo p. Sie sind paarweise inkongruent modulo p, denn aus $\lambda^2 \equiv \mu^2 \bmod p$ folgt $p \mid (\lambda - \mu)$ oder $p \mid (\lambda + \mu)$. Wegen $1 < \lambda + \mu < p$ entfällt die zweite Möglichkeit, und aus $|\lambda - \mu| < p$ folgt $\lambda = \mu$.
b) Zu zeigen bleibt, daß es keine weiteren quadratischen Reste modulo p gibt. Sämtliche quadratischen Reste modulo p sind unter den Restklassen $m^2 \mod p$ mit $1 \leq m \leq p-1$.

Wegen $\nu^2 \equiv (p-\nu)^2 \bmod p$ kann es nur höchstens $\frac{p-1}{2}$ quadratische Reste modulo p geben, und die Behauptung folgt aus a). □

Satz 2. Es besteht das Eulersche Kriterium: Für $2 \neq p \in \mathbb{P}$ gilt

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

Beweis. Für $p \mid a$ ist die Behauptung offenbar richtig. Es sei nun $p \nmid a$. Wir unterscheiden zwei Fälle.
a) $\left(\frac{a}{p}\right) = 1$: Dann existiert ein $\xi \in \mathbb{Z}$ mit $\xi^2 \equiv a \bmod p$, und der kleine Fermatsche Satz liefert wegen $p \nmid \xi$

$$a^{\frac{p-1}{2}} \equiv \xi^{p-1} \equiv 1 \bmod p.$$

b) $\left(\frac{a}{p}\right) = -1$: Der kleine Fermatsche Satz liefert $p \mid (a^{p-1}-1)$, also $p \mid (a^{\frac{p-1}{2}}-1)$ oder $p \mid (a^{\frac{p-1}{2}}+1)$. Im letzten Fall folgt $a^{\frac{p-1}{2}} \equiv -1 \bmod p$ und daraus die Behauptung. Zu zeigen bleibt, daß der erste Fall unmöglich ist. Angenommen, es gilt doch $p \mid (a^{\frac{p-1}{2}}-1)$. Dann hat die Kongruenz $x^{\frac{p-1}{2}} \equiv 1 \bmod p$ die Lösungen $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$. Diese Zahlen sind paarweise inkongruent modulo p. Außerdem ist a eine Lösung der obigen Kongruenz. Da a quadratischer Nichtrest modulo p ist, haben wir damit $\frac{p+1}{2}$ paarweise inkongruente Lösungen von $x^{\frac{p-1}{2}} \equiv 1 \bmod p$. Dies widerspricht dem Satz von Lagrange (Kapitel 4, Satz 5). □

Satz 3. Für $2 \neq p \in \mathbb{P}$ und alle $a, b \in \mathbb{Z}$ gilt $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$; das Legendre-Symbol nach p ist also eine vollständig multiplikative Funktion.

Beweis. Das Euler-Kriterium liefert

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

Es folgt

$$p \,\Big|\, \left(\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\right).$$

Dabei ist der Betrag der rechten Seite ≤ 2, wegen $p > 2$ also Null, und die Kongruenz modulo p geht in Gleichheit über. □

Folgerung 2. Reste und Nichtreste modulo p genügen dem Multiplikationsschema

$$\mathrm{R} \times \mathrm{R} = \mathrm{N} \times \mathrm{N} = \mathrm{R} \quad \text{und} \quad \mathrm{R} \times \mathrm{N} = \mathrm{N} \times \mathrm{R} = \mathrm{N}\,.$$

Die Bestimmung von $\left(\frac{a}{p}\right)$ braucht nur durchgeführt zu werden für $a = -1$, $a = 2$ und $a = q \in \mathbb{P}$ mit ungeraden Primzahlen $p \neq q$.

Nachweis. Die Behauptungen folgen aus Satz 3. □

5.2 Die Ergänzungssätze und das Gaußsche Lemma

Satz 4. (1. Ergänzungssatz) Für $2 \neq p \in \mathbb{P}$ gilt $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Beweis. Das Euler-Kriterium liefert $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p$, woraus wie bei Satz 3 die Behauptung folgt. □

Folgerung 3. Die Kongruenz $x^2 + 1 \equiv 0 \bmod p$ ist lösbar genau für die Primzahlen $p = 2$ und $p \equiv 1 \bmod 4$.

Folgerung 4. Es gibt unendlich viele Primzahlen $p \equiv 1 \bmod 4$.

Nachweis. Euklids Idee läßt sich modifizieren: Angenommen, es sind $p_1, \ldots, p_k$ sämtliche Primzahlen $\equiv 1 \bmod 4$. Die Zahl

$$n = (2p_1 \cdot \ldots \cdot p_k)^2 + 1 > 1$$

besitzt einen Primteiler p. Offenbar gilt $p \notin \{2, p_1, \ldots, p_k\}$. Es folgt $p \equiv 3 \bmod 4$ im Widerspruch zu Folgerung 3. □

Satz 5. (Gausssches Lemma) Es sei $2 \neq p \in \mathbb{P}$ und $p \nmid a \in \mathbb{Z}$. Es bezeichne ν die Anzahl der Zahlen $1a, 2a, \ldots, \frac{p-1}{2}a$, deren absolut kleinster Rest modulo p negativ ist. Dann gilt

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

Beweis. Die absolut kleinsten primen Reste modulo p sind die $p-1$ Zahlen $\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}$. Sie bilden ein primes Restsystem modulo p. Die absolut kleinsten Reste modulo p der Zahlen $1a, 2a, \ldots, \frac{p-1}{2}a$ seien, gegebenenfalls in anderer Reihenfolge,

$$-r_1, -r_2, \ldots, -r_\nu;\ r'_1, r'_2, \ldots, r'_\lambda \qquad (0 < r_i, r'_j \leq \tfrac{p-1}{2})$$

mit $\nu + \lambda = \frac{p-1}{2}$. Sie besitzen die Eigenschaften

$$\begin{aligned} i \neq j \quad &\Longrightarrow \quad r_i \not\equiv r_j \bmod p, \\ i \neq j \quad &\Longrightarrow \quad r'_i \not\equiv r'_j \bmod p, \\ i, j \geq 1 \quad &\Longrightarrow \quad r_i \not\equiv r'_j \bmod p. \end{aligned}$$

Nur die letzte Eigenschaft ist nichttrivial. Sie wird indirekt gezeigt: Angenommen, es gilt doch $r_i \equiv r'_j \bmod p$ für gewisse i, j. Dann folgt $p - r_i + r'_j \equiv 0 \bmod p$. Die Zahlen $p - r_i$ und r'_j sind Reste von verschiedenen Vielfachen ϱa und $\sigma a \bmod p$. Das heißt, es gilt $p \mid (\varrho + \sigma)a$, wegen $p \nmid a$ also $p \mid (\varrho + \sigma)$. Das ist wegen $1 < \varrho + \sigma < p$ unmöglich.

Damit ist gezeigt: Die $\frac{p-1}{2}$ Zahlen r_i, r'_j bilden eine Permutation der Zahlen $1, \ldots, \frac{p-1}{2}$. Es folgt

$$r_1 \cdots r_\nu \cdot r'_1 \cdots r'_\lambda = \Big(\frac{p-1}{2}\Big)!$$

und weiter

$$a^{\frac{p-1}{2}} \Big(\frac{p-1}{2}\Big)! \equiv (-1)^{\nu} \Big(\frac{p-1}{2}\Big)! \bmod p\,.$$

Das ergibt

$$a^{\frac{p-1}{2}} \equiv (-1)^{\nu} \bmod p,$$

mit dem Euler-Kriterium also

$$\left(\frac{a}{p}\right) \equiv (-1)^{\nu} \bmod p,$$

woraus die Behauptung folgt. □

Eine erste Anwendung des Gaußschen Lemmas ist der

Satz 6. (2. Ergänzungssatz) Für $2 \neq p \in \mathbb{P}$ gilt $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Beweis. Wir setzen $a = 2$ im Gaußschen Lemma und müssen die negativen unter den absolut kleinsten Resten modulo p der Zahlen $2, 4, \ldots, p-1$ abzählen. Man sieht sofort $\lambda = \left[\frac{p-1}{4}\right]$, also

$$\nu = \frac{p-1}{2} - \left[\frac{p-1}{4}\right].$$

Zu zeigen bleibt: $\frac{p-1}{2} - \left[\frac{p-1}{4}\right] \equiv \frac{p^2-1}{8} \bmod 2$.

Für $p \equiv 1 \bmod 4$, also $p = 4k+1$ mit $k \in \mathbb{N}$ folgt

$$\frac{p-1}{2} - \left[\frac{p-1}{4}\right] = k \quad \text{und} \quad \frac{p^2-1}{8} = 2k^2 + k \equiv k \bmod 2.$$

Für $p \equiv -1 \bmod 4$, also $p = 4k-1$ mit $k \in \mathbb{N}$ folgt

$$\frac{p-1}{2} - \left[\frac{p-1}{4}\right] = k \quad \text{und} \quad \frac{p^2-1}{8} = 2k^2 - k \equiv k \bmod 2.$$

Damit ist Satz 6 bewiesen. □

Bemerkung 2. Nur eine andere Formulierung von Satz 6 ist

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{für } p \equiv \pm 1 \bmod 8 \\ -1 & \text{für } p \equiv \pm 3 \bmod 8. \end{cases}$$

Die quadratische Kongruenz $x^2 \equiv 2 \bmod p$ ist also lösbar genau für die Primzahlen $p = 2$ und $p \equiv \pm 1 \bmod 8$.

Folgerung 5. (Euler) Es seien $p \equiv 3 \bmod 4$ und $q = 2p+1$ Primzahlen. Dann gilt $2^p - 1 \equiv 0 \bmod q$. Insbesondere ist $2^p - 1$ nicht Primzahl, wenn $q = 2p+1 \in \mathbb{P}$ mit einer Primzahl $p > 3$ besteht.

Nachweis. Es gilt $q \equiv 7 \bmod 8$, infolge Satz 6 also $\left(\frac{2}{q}\right) = 1$. Das Euler-Kriterium liefert

$$1 = \left(\frac{2}{q}\right) \equiv 2^{\frac{q-1}{2}} \equiv 2^p \bmod q,$$

wie behauptet. Der Zusatz kommt aus $2^p - 1 > 2p + 1 = q$ für $p > 3$, so daß q dann echter Teiler von $2^p - 1$ ist. □

Beispiel 2. Die Mersenneschen Zahlen $2^{11} - 1$, $2^{23} - 1$ sind nicht prim, denn $23 \mid 2^{11} - 1$ und $47 \mid 2^{23} - 1$.

5.3 Das quadratische Reziprozitätsgesetz

Satz 7. (Quadratisches Reziprozitätsgesetz) Für ungerade Primzahlen $p \neq q$ gilt

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

Beweis. Wir setzen $p = 2k+1$, $q = 2\ell+1$ und bestimmen $\left(\frac{q}{p}\right)$ mit dem Gaußschen Lemma. Zu betrachten sind die Zahlen $1q, 2q, \ldots, kq$. Für $1 \leq \kappa \leq k$ gilt $\kappa q = \left[\frac{\kappa q}{p}\right]p + \varrho_\kappa$ mit $1 \leq \varrho_\kappa \leq p-1$. Summation ergibt

$$q\,\frac{k(k+1)}{2} = p\sum_{\kappa=1}^{k}\left[\frac{\kappa q}{p}\right] + \sum_{\kappa=1}^{k}\varrho_\kappa\,.$$

Die Beträge $|r_\kappa|$ der absolut kleinsten $r_\kappa \equiv \varrho_\kappa \bmod p$ durchlaufen die Zahlen von 1 bis k. Es sei wieder ν die Anzahl der negativen unter den r_κ. Dann gilt

$$\sum_{\kappa=^1}^{k}\varrho_\kappa = \nu p + \sum_{\kappa=1}^{k} r_\kappa\,,$$

also

$$q\,\frac{k(k+1)}{2} = p\sum_{\kappa=1}^{k}\left[\frac{\kappa q}{p}\right] + \nu p + \sum_{\kappa=1}^{k} r_\kappa\,.$$

Nach dem Gaußschen Lemma gilt $\left(\frac{q}{p}\right) = (-1)^\nu$, und es kommt nur darauf an zu entscheiden, ob ν gerade oder ungerade ist. Daher braucht die obige Gleichung nur modulo 2 ausgewertet zu werden. Wegen $x \equiv -x \bmod 2$ für jedes $x \in \mathbb{Z}$ folgt

$$\frac{k(k+1)}{2} \equiv \sum_{\kappa=1}^{k}\left[\frac{\kappa q}{p}\right] + \nu + \sum_{\kappa=1}^{k}|r_\kappa| \bmod 2.$$

Darin hat die letzte Summe den Wert $\frac{k(k+1)}{2}$, und es kommt

$$\nu \equiv \sum_{\kappa=1}^{k}\left[\frac{\kappa q}{p}\right] \bmod 2.$$

Für $\left(\frac{p}{q}\right) = (-1)^\sigma$ folgt analog

$$\sigma \equiv \sum_{\lambda=1}^{\ell}\left[\frac{\lambda p}{q}\right] \bmod 2.$$

Demnach ist Satz 7 vollständig bewiesen, wenn gezeigt wird, daß $\nu + \sigma \equiv k\ell \bmod 2$ besteht, also

$$\sum_{\kappa=1}^{k}\left[\frac{\kappa q}{p}\right] + \sum_{\lambda=1}^{\ell}\left[\frac{\lambda p}{q}\right] \equiv k\ell \bmod 2.$$

Wir zeigen sogar

$$\sum_{\kappa=1}^{k} \left[\frac{\kappa q}{p}\right] + \sum_{\lambda=1}^{\ell} \left[\frac{\lambda p}{q}\right] = k\ell. \tag{2}$$

Dazu betrachten wir die Zahlen $\kappa q - \lambda p$ mit $1 \leq \kappa \leq k$ und $1 \leq \lambda \leq \ell$. Es sind $k\ell$ paarweise verschiedene Zahlen $\neq 0$. Wir zählen die positiven unter ihnen ab: Bei festem κ sind es genau $\left[\frac{\kappa q}{p}\right]$, insgesamt ist also genau

$$\sum_{\kappa=1}^{k} \left[\frac{\kappa q}{p}\right].$$

Wir zählen die negativen unter ihnen ab: Es sind genau

$$\sum_{\lambda=1}^{\ell} \left[\frac{\lambda p}{q}\right].$$

Addition ergibt die Restbehauptung (2). Damit ist Satz 7 bewiesen. □

Beispiel 3. Ist die Kongruenz $x^2 \equiv 300 \bmod 101$ lösbar?

Es gilt

$$\left(\frac{300}{101}\right) = \left(\frac{3}{101}\right)\left(\frac{100}{101}\right) = \left(\frac{3}{101}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{101-1}{2}}\left(\frac{101}{3}\right) = \left(\frac{101}{3}\right) = \left(\frac{-1}{3}\right) = -1,$$

die Kongruenz $x^2 \equiv 300 \bmod 101$ ist also unlösbar.

Beispiel 4. Für welche Primzahlen ist $x^2 \equiv 3 \bmod p$ lösbar?

Für $p = 2$ und $p = 3$ ist die Lösbarkeit trivial. Für $p > 3$ heißt Lösbarkeit $\left(\frac{3}{p}\right) = 1$. Das quadratische Reziprozitätsgesetz liefert

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

Wir unterscheiden zwei Fälle:

Es ist $\left(\frac{p}{3}\right) = 1$ und $(-1)^{\frac{p-1}{2}} = 1$ äquivalent zu $p \equiv 1 \bmod 3$ und $p \equiv 1 \bmod 4$, also zu $p \equiv 1 \bmod 12$; es ist $\left(\frac{p}{3}\right) = -1$ und $(-1)^{\frac{p-1}{2}} = -1$ äquivalent zu $p \equiv -1 \bmod 3$ und $p \equiv -1 \bmod 4$, also zu $p \equiv -1 \bmod 12$. Insgesamt ist $x^2 \equiv 3 \bmod p$ ist lösbar genau für die Primzahlen $p = 2$, $p = 3$ und $p \equiv \pm 1 \bmod 12$.

Leicht zu sehen ist damit, daß $x^2 \equiv 3 \bmod p^k$ mit $1 < k \in \mathbb{N}$ lösbar genau für die Primzahlen $p \equiv \pm 1 \bmod 12$ ist.

Bemerkung 3. Für $k \in \mathbb{N}$, $a \in \mathbb{Z}$ und $p \in \mathbb{P}$ mit $p \nmid 2a$ ist $x^2 \equiv a \bmod p^k$ lösbar genau dann, wenn $\left(\frac{a}{p}\right) = 1$ gilt.

Kapitel 6

Summen von Quadraten

Das Ziel dieses Kapitels ist die multiplikative Charakterisierung der natürlichen Zahlen, die eine Darstellung als Summe von höchstens zwei Quadratzahlen besitzen, sowie der Nachweis, daß jede natürliche Zahl eine Summe von höchstens vier Quadratzahlen ist.

6.1 Summen von zwei Quadraten

Für festes $k \in \mathbb{N}$ setzen wir

$$Q_k = \{n \in \mathbb{N} : \text{ es existieren } n_1, \ldots, n_k \in \mathbb{N}_0 \text{ mit } n = n_1^2 + \ldots + n_k^2\}.$$

Offenbar gilt $Q_1 \subset Q_2 \subset Q_3 \subset Q_4 \subseteq \ldots$ wegen $2 \in Q_2 \setminus Q_1$, $3 \in Q_3 \setminus Q_2$ und $7 \in Q_4 \setminus Q_3$. Hier wird Q_2 charakterisiert. Eine wichtige multiplikative Eigenschaft enthält

Lemma 1. Aus $m, n \in Q_2$ folgt $mn \in Q_2$.

Beweis. Es gilt, wie man leicht direkt verifiziert,

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

Aufschlußreicher ist der komplexe Beweis. Es gilt nämlich $(a-bi)(c+di) = (ac+bd)+i(ad-bc)$, und die Norm $N(z) := |z|^2 = z\overline{z}$ hat die Eigenschaft $N(zw) = N(z)N(w)$. Daraus folgt die Behauptung. □

Wir untersuchen, welche Primzahlen in Q_2 liegen.

Lemma 2. Es gilt $2 \in Q_2$ sowie $p \in Q_2$ für alle $p \in \mathbb{P}$ mit $p \equiv 1 \bmod 4$.

Beweis. Klar ist $1^2 + 1^2 = 2 \in Q_2$. Für $p \in \mathbb{P}$, $p \equiv 1 \bmod 4$, ist die Kongruenz $x^2 + 1 \equiv 0 \bmod p$ lösbar durch ein $x \in \mathbb{N}$ mit $1 \leq x < \frac{p}{2}$. Erst recht ist $x^2 + y^2 \equiv 0 \bmod p$ lösbar durch

ein Paar $(x, y) \in \mathbb{N}^2$ mit $1 \leq x, y < \frac{p}{2}$. Es sei jetzt $(x_0\,,\, y_0)$ ein Lösungspaar derart, daß

$$x_0^2 + y_0^2 = m_0\, p \qquad \big(1 \leq x_0\,,\, y_0 < \frac{p}{2}\big) \tag{1}$$

mit minimalen $m_0 \in \mathbb{N}$ besteht. Dann sind $x_0\,,\, y_0$ teilerfremd, und es gilt $1 \leq m_0 < p$. Wir zeigen $m_0 = 1$.

Angenommen, es gilt $m_0 > 1$. Division von $x_0\,,\, y_0$ durch m_0 mit kleinstem Absolutrest liefert die Existenz von $\lambda, \mu \in \mathbb{N}_0$ mit

$$x_0 = \lambda m_0 + x_1\,, \quad y_0 = \mu m_0 + y_1 \qquad \big(|x_1|, |y_1| \leq \frac{m_0}{2}\big).$$

Es gilt $x_1^2 + y_1^2 > 0$, denn aus $x_1 = y_1 = 0$ folgt $m_0 \mid (x_0\,,\, y_0) = 1$, also schon $m_0 = 1$ entgegen der Annahme. Wir haben damit $0 < x_1^2 + y_1^2 \equiv x_0^2 + y_0^2 \equiv 0 \bmod m_0$ oder

$$x_1^2 + y_1^2 = m_1 m_0 \qquad \big(0 < m_1 < m_0\big). \tag{2}$$

Multiplikation von (1) und (2) ergibt $m_1 m_0^2 p = (x_0^2 + y_0^2)(x_1^2 + y_1^2)$. Mit der Zerlegungsformel aus Lemma 1 geht dies über in

$$m_1 m_0^2\, p = (x_0 x_1 + y_0 y_1)^2 + (x_0 y_1 - x_1 y_0)^2. \tag{3}$$

Dabei gilt

$$\begin{aligned} x_0 x_1 + y_0 y_1 &= x_0(x_0 - \lambda m_0) + y_0(y_0 - \mu m_0) = m_0(p - \lambda x_0 - \mu y_0) = m_0\, x_2\,, \\ x_0 y_1 - x_1 y_0 &= x_0(y_0 - \mu m_0) - y_0(x_0 - \lambda m_0) = m_0(\lambda y_0 - \mu x_0) = m_0\, y_2\,, \end{aligned}$$

und aus (3) entsteht

$$m_1\, p = x_2^2 + y_2^2$$

mit $0 < m_1 < m_0$. Das ist der Widerspruch zur Minimalität von m_0. Es folgt $m_0 = 1$, und Lemma 2 ist vollständig bewiesen. □

Lemma. 3. Es sei $n \in Q_2$ und $p^\nu \| n$ mit $p \in \mathbb{P}$, $p \equiv 3 \bmod 4$, $\nu \in \mathbb{N}$. Dann gilt $2 \mid \nu$.

Beweis. Jedes $n \in Q_2$ läßt sich in der Form $n = m^2(a^2 + b^2)$ mit teilerfremden $a, b \in \mathbb{N}_0$ schreiben. Wir zeigen $p \nmid (a^2 + b^2)$, woraus $p^\nu \| m^2$ und weiter $2 \mid \nu$ folgt.

Angenommen, es gilt doch $a^2 + b^2 \equiv 0 \bmod p$. Wegen $(a, b) = 1$ folgt $p \nmid b$. Also existiert $b' \in \mathbb{N}$ mit $bb' \equiv 1 \bmod p$, also $(ab')^2 + 1 \equiv 0 \bmod p$. Das heißt, daß die Kongruenz $x^2 \equiv -1 \bmod p$ lösbar ist entgegen $\left(\frac{-1}{p}\right) = -1$ für Primzahlen $p \equiv 3 \bmod 4$. □

Zusammenfassung der drei Lemmata ergibt den

Satz 1. (Fermat) Eine natürliche Zahl ist genau dann Summe von höchstens zwei Quadratzahlen, wenn ihre Primteiler $p \equiv 3 \bmod 4$ in gerader Multiplizität in ihr aufgehen.

Bemerkung 1. Es gilt $Q_2 = \{km^2 \in \mathbb{N} : p \mid k \Longrightarrow p = 2 \text{ oder } p \equiv 1 \bmod 4\}$.

6.2 Summen von vier Quadraten

Man sieht leicht, daß keine Zahl der Form $4^\lambda(8k+7)$ mit $\lambda, k \in \mathbb{N}_0$ in Q_3 liegt. Daß umgekehrt Q_3 aus allen anderen natürlichen Zahlen besteht, ist schwieriger zu beweisen. Es werden dazu Kenntnisse aus der Theorie der ternären quadratischen Formen benötigt. Eine Lemma 1 entsprechende multiplikative Charakterisierung von Q_3 gibt es nicht, wie das Bespiel der Zahlen $3, 5 \in Q_3$ zeigt; es gilt $15 \notin Q_3$. Der Vier-Quadrate-Satz von Lagrange besagt $Q_4 = \mathbb{N}$:

Satz 2. (Lagrange) Jede natürliche Zahl ist Summe von höchstens vier Quadratzahlen.

Bemerkung 2. Zusammen mit $Q_3 \neq Q_4$ liefert Satz 2 die Lösung des Waringschen Problems für Quadratzahlen. Es gilt $g(2) = 4$ (vgl. Beispiel 7 aus Kapitel 1).

Zum Beweis von Satz 2 benötigen wir eine multiplikative Charakterisierung von Q_4 .

Lemma 4. Aus $m, n \in Q_4$ folgt $mn \in Q_4$.

Beweis. Es besteht die Eulersche Identität

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)\,(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2 \tag{4}$$

mit

$$\begin{cases} z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\ z_2 = x_1y_2 - x_2y_1 - x_3y_4 - x_4y_3 \\ z_3 = x_1y_3 + x_2y_4 - x_3y_1 - x_4y_2 \\ z_4 = x_1y_4 - x_2y_3 + x_3y_2 - x_4y_1. \end{cases} \tag{5}$$

Diese Identität läßt sich direkt verifizieren, aber wie kommt man darauf? Hierzu ist etwas Algebra nützlich: Der Quaternionenschiefkörper $\mathbb{H}$ (nach Hamilton, 1805 - 1865, der ihn zuerst systematisch untersuchte) entsteht aus $\mathbb{R}$ durch Adjunktion von i, j, k mit

$$i^2 = j^2 = k^2 = -1\,; \quad ij = k = -ji\,,\ jk = i = -kj\,,\ ki = j = -ik\,.$$

In

$$\mathbb{H} = \{x_1 + x_2i + x_3j + x_4k : x_1\,,\ x_2\,,\ x_3\,,\ x_4 \in \mathbb{R}\}$$

läßt sich mit der Addition wie in $\mathbb{R}^4$ und der Multiplikation gemäß obigen Regeln vernünftig rechnen. Man addiert komponentenweise und multipliziert gemäß

$$(x_1 - x_2i - x_3j - x_4k)(y_1 + y_2i + y_3j + y_4k) = z_1 + z_2i + z_3j + z_4k$$

mit den Zahlen $z_1\,,\ z_2\,,\ z_3\,,\ z_4 \in \mathbb{R}$ aus (5). Die Multiplikation ist offenbar nicht kommutativ. Die Existenz von $(\mathbb{H},\ +,\ \cdot\,)$ ergibt sich konstruktiv aus der Existenz von $\mathbb{R}^4$. Setzt man die zu $X = x_1 + x_2i + x_3j + x_4k$ konjugierte Zahl $\overline{X}$ durch

$$\overline{X} = x_1 - x_2i - x_3j - x_4k$$

fest, so folgt $X\overline{X} = \overline{X}X = x_1^2 + x_2^2 + x_3^2 + x_4^2 \in \mathbb{R}$. Das Produkt $N(X) := X\overline{X}$ nennt man die Norm von X. Sie ist multiplikativ, $N(XY) = N(X)\,N(Y)$, was aus $\overline{XY} = \overline{X}\,\overline{Y}$ folgt. Die Beziehungen (4) und (5) lauten dann kürzer $N(X)\,N(Y) = N(Z)$ mit $Z = \overline{X}\,Y$. □

Die zahlentheoretische Konsequenz von Lemma 4 besteht darin, daß zum vollständigen Beweis von Satz 2 nur noch gezeigt werden muß, daß jede Primzahl eine Darstellung als Summe von höchstens vier Quadratzahlen besitzt. Aus Lemma 2 wissen wir das schon für $p = 2$ und $p \equiv 1 \bmod 4$. Es bringt aber keinen Vorteil, nur die Primzahlen $p \equiv 3 \bmod 4$ zu betrachten.

Beweis von Satz 2. Wegen Lemma 4 genügt es, $p \in Q_4$ für alle ungeraden $p \in \mathbb{P}$ zu zeigen.

a) Wir zeigen zuerst die Existenz von $x, y \in \mathbb{N}_0$ mit $0 \le x, y < \frac{p}{2}$ und

$$x^2 + y^2 + 1 \equiv 0 \bmod p.$$

Denn die $\frac{p+1}{2}$ Zahlen x^2 mit $0 \le x \le \frac{p-1}{2}$ sind paarweise inkongruent mod$p$, und die $\frac{p+1}{2}$ Zahlen $-y^2-1$ mit $0 \le p \le \frac{p-1}{2}$ sind auch paarweise inkongruent $\bmod p$. Von diesen insgesamt $p+1$ Zahlen fallen wenigstens zwei in dieselbe Restklasse $\bmod p$. Damit folgt die Existenz von x, y mit $0 \le x \le \frac{p-1}{2}$ und $x^2 \equiv -1 - y^2 \bmod p$.

b) Wegen a) existieren Zahlen $x_1\,,\ x_2\,,\ x_3\,,\ x_4 \in \mathbb{Z}$ mit $|x_\nu| < \frac{p}{2}$, so daß gilt

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0\, p \tag{6}$$

mit minimalem $m_0 \in \mathbb{N}$. Dann besteht $1 \le m_0 < p$ sowie $(x_1\,,\ x_2\,,\ x_3\,,\ x_4) = 1$.

c) Wir zeigen nun $m_0 = 1$. Angenommen, es gilt $m_0 > 1$. Aus (6) folgt speziell

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \bmod m_0\,,$$

und hierin sind wegen $(x_1\,,\ x_2\,,\ x_3\,,\ x_4) = 1 < m_0$ nicht alle x_ν durch m_0 teilbar. Division von x_ν mit kleinstem Absolutrest durch m_0 liefert die Existenz von Zahlen $\lambda_\nu \in \mathbb{N}_0$ und $y_\nu \in \mathbb{Z}$ mit

$$x_\nu = \lambda_\nu m_0 + y_\nu\,, \quad |y_\nu| \le \frac{m_0}{2}\,.$$

Es folgt $0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \bmod m_0$ oder

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_0\, m_1 \quad \text{mit} \quad 0 < m_1 \le m_0\,. \tag{7}$$

Wir schließen $m_1 = m_0$ aus: In diesem Fall gilt nämlich $|y_1| = |y_2| = |y_3| = |y_4| = \frac{m_0}{2}$, insbesondere $2 \mid m_0$ und $x_\nu = (2\lambda_\nu \pm 1)\,\frac{m_0}{2}$. Einsetzen in (6) ergibt

$$\frac{m_0^2}{4}\,\left((2\lambda_1 \pm 1)^2 + (2\lambda_2 \pm 1)^2 + (2\lambda_3 \pm 1)^2 + (2\lambda_4 \pm 1)^2\right) = m_0\, p$$

oder

$$\frac{m_0}{2} \cdot \frac{1}{2}\left((2\lambda_1 \pm 1)^2 + (2\lambda_2 \pm 1)^2 + (2\lambda_3 \pm 1)^2 + (2\lambda_4 \pm 1)^2\right) = p.$$

Wegen $p \in \mathbb{P}$ folgt $m_0 = 2$. Deshalb sind alle x_ν ungerade. Aus (6), also $x_1^2+x_2^2+x_3^2+x_4^2 = 2p$, kommt aber

$$\left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2 = p.$$

Dies widerspricht der Minimalität von m_0. Es folgt daher $m_1 < m_0$, wie behauptet. Multiplikation der Gleichungen (6) und (7) ergibt

$$m_1\, m_0^2\, p = (x_1^2 + x_2^2 + x_3^2 + x_4^2)\,(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

mit den Zahlen z_ν aus (5). Wir werden nachrechnen, daß jede der Zahlen z_ν durch m_0 teilbar ist. Dann gilt also $z_\nu = m_0 t_\nu$ mit $t_\nu \in \mathbb{Z}$, und es folgt

$$m_1 p = t_1^2 + t_2^2 + t_3^2 + t_4^2 \,.$$

Dies widerspricht der Minimalität von $m_0 > 1$. Es gilt also $m_0 = 1$ in (6), und Satz 2 ist nachgewiesen. Die letzte Rechenaufgabe ist rasch erledigt: Aus den Gleichungen (5), (6), (7) kommt

$$\begin{aligned}
z_1 &\equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \bmod m_0 \\
z_2 &\equiv x_1 x_2 - x_2 x_1 - x_3 x_4 + x_4 x_3 \equiv 0 \bmod m_0 \\
z_3 &\equiv x_1 x_3 + x_2 x_4 - x_3 x_1 - x_4 x_2 \equiv 0 \bmod m_0 \\
z_4 &\equiv x_1 x_4 - x_2 x_3 + x_3 x_2 - x_4 x_1 \equiv 0 \bmod m_0 .
\end{aligned}$$

□

Bemerkung 4. Die vorstehenden Beweise der Sätze 1 und 2 sind ähnlich. Sie beruhen beide auf der von Fermat entwickelten „Methode des Abstiegs“. Es gibt inzwischen andere Beweismethoden für den Kern der beiden Sätze, daß nämlich jede Primzahl $\equiv 1 \bmod 4$ Summe von zwei Quadraten und jede Primzahl $\equiv 3 \bmod 4$ Summe von vier Quadraten ist.

Kapitel 7

Arithmetische Funktionen

In diesem Kapitel wird die arithmetische Struktur komplexwertiger Folgen erörtert.

7.1 Die Dirichletsche Faltung

Definition. Jede Folge $f : \mathbb{N} \to \mathbb{C}$ heißt arithmetische Funktion. Ihre Menge wird mit $\mathcal{F}$ bezeichnet. Auf $\mathcal{F}$ sind die linearen Operationen für $f, g \in \mathcal{F}$ und $\lambda \in \mathbb{C}$ wie üblich punktweise durch

$$(f+g)(n) = f(n) + g(n) \quad \text{und} \quad (\lambda f)(n) = \lambda f(n)$$

und die Dirichletsche Faltung $*$ durch

$$(f * g)(n) = \sum_{\substack{d,m \in \mathbb{N} \\ dm = n}} f(d)\, g(m) \qquad (n \in \mathbb{N})$$

erklärt.

Hinsichtlich der linearen Operationen bildet $\mathcal{F}$ ersichtlich einen $\mathbb{C}$-linearen Raum (komplexen Vektorraum). Hinsichtlich der Addition und der Dirichletschen Faltung als multiplikativer Verknüpfung ist $\mathcal{F}$ ein Integritätsbereich, also ein kommutativer nullteilerfreier Ring mit Einselement $\varepsilon \in \mathcal{F}$,

$$\varepsilon(n) = \begin{cases} 1 & \text{für } n = 1 \\ 0 & \text{sonst} \end{cases} \qquad (n \in \mathbb{N}).$$

Die Nullteilerfreiheit sieht man so: Aus $f(a) \neq 0$ und $g(b) \neq 0$ mit minimalen Zahlen $a, b \in \mathbb{N}$ folgt $(f * g)(ab) = f(a)\, g(b) \neq 0$. Diese Eigenschaften faßt der folgende Satz zusammen.

Satz 1. Unter den linearen Operationen und der Dirichletschen Faltung bildet $\mathcal{F}$ eine kommutative $\mathbb{C}$-Algebra mit Eins.

Es stellt sich die Frage nach der multiplikativen Gruppe $\mathcal{F}^*$ von $\mathcal{F}$; sie besteht aus den bezüglich der Dirichletschen Faltung invertierbaren Elementen von $\mathcal{F}$.

Satz 2. Die multiplikative Gruppe von $\mathcal{F}$ ist $\mathcal{F}^* = \{f \in \mathcal{F} : f(1) \neq 0\}$.

Beweis. Nach Definition enthält $\mathcal{F}^*$ genau solche $f \in \mathcal{F}$, zu denen es ein $g \in \mathcal{F}$ mit $f * g = \varepsilon$ gibt. Das heißt

$$\sum_{\substack{d,m\in\mathbb{N}\\ dm=n}} f(d)\,g(m) = \begin{cases} 1 & \text{für } n = 1 \\ 0 & \text{sonst.} \end{cases}$$

Dies ist ein unendliches lineares Gleichungssystem für die Werte von g auf $\mathbb{N}$. Es ist eindeutig lösbar genau für $f(1) \neq 0$, nämlich durch

$$g(n) = \begin{cases} \frac{1}{f(1)} & \text{für } n = 1 \\ -\frac{1}{f(1)} \sum\limits_{\substack{dm=n\\ m<n}} f(d)\,g(m) & \text{sonst.} \end{cases}$$

Wegen $(f * g)(1) = f(1)\,g(1)$ ist $\mathcal{F}^*$ auch abgeschlossen unter der Dirichletschen Faltung, insgesamt also Gruppe. □

Das faltungsinverse Element von $f \in \mathcal{F}^*$ wird fortan mit f^{-1} bezeichnet. Die Rekursionsgleichung für f^{-1} führt im allgemeinen *nicht* zu einer expliziten Formel für die Werte $f^{-1}(n)$.

Eine andere multiplikative Verknüpfung auf $\mathcal{F}$ ist das punktweise Produkt $fg \in \mathcal{F}$ von $f, g \in \mathcal{F}$. Diese Operation macht zusammen mit der punktweisen Addition aus $\mathcal{F}$ einen *nicht* nullteilerfreien kommutativen Ring mit Einselement $1 \in \mathcal{F}$, definiert durch $1(n) = 1$ für alle $n \in \mathbb{N}$. Dessen multiplikative Gruppe ist die Menge der $f \in \mathcal{F}$ mit $f(n) \neq 0$ für alle $n \in \mathbb{N}$.

Als einfache gruppentheoretische Konsequenz von Satz 2 notieren wir

Folgerung 1. Es seien $f, g \in \mathcal{F}$ und $h \in \mathcal{F}^*$. Dann sind die Beziehungen $f = g * h$ und $g = f * h^{-1}$ äquivalent.

Folgerung 2. Es seien $F, G : [1, \infty) \to \mathbb{C}$ und $h \in \mathcal{F}^*$. Dann sind äquivalent:

(i) $$F(x) = \sum_{d\le x} h(d)\,G\Big(\frac{x}{d}\Big) \quad \text{für alle } x \ge 1\,,$$

(ii) $$G(x) = \sum_{d\le x} h^{-1}(d)\,F\Big(\frac{x}{d}\Big) \quad \text{für alle } x \ge 1\,.$$

Nachweis. Es genügt zu zeigen, daß (ii) aus (i) folgt. Dazu rechnen wir nach,

$$\begin{aligned}\sum_{d\le x} h^{-1}(d)\,F\Big(\frac{x}{d}\Big) &= \sum_{d\le x} h^{-1}(d) \sum_{m\le x/d} h(m)\,G\Big(\frac{x}{dm}\Big) = \sum_{dm\le x} h^{-1}(d)\,h(m)\,G\Big(\frac{x}{dm}\Big) \\ &= \sum_{n\le x} \Big(\sum_{dm=n} h^{-1}(d)\,h(m)\Big)\,G\Big(\frac{x}{n}\Big) = \sum_{n\le x} G\Big(\frac{x}{n}\Big) = G(x)\,,\end{aligned}$$

wie in (ii) behauptet. □

7.2 Additive und multiplikative Funktionen

Von besonderem Interesse sind arithmetische Funktionen, die zusätzliche additive oder multiplikative Eigenschaften aufweisen und oft vorkommen.

Definition. Funktionen $f \in \mathcal{F}$ heißen additiv, wenn gilt

(1) $$f(mn) = f(m) + f(n) \qquad \text{für alle teilerfremden } m, n \in \mathbb{N}.$$

Funktionen $f \in \mathcal{F}^*$ heißen multiplikativ, wenn gilt

(2) $$f(mn) = f(m)\, f(n) \qquad \text{für alle teilerfremden } m, n \in \mathbb{N}.$$

Die Mengen der additiven und der multiplikativen Funktionen werden mit $\mathcal{A}$ bzw. mit $\mathcal{M}$ bezeichnet. Gelten die Gleichungen (1) bzw. (2) sogar für alle $m, n \in \mathbb{N}$, so heißen $f \in \mathcal{F}$ bzw. $f \in \mathcal{F}^*$ vollständig additiv bzw. vollständig multiplikativ.

Beispiel 1. Es sei $\omega(n)$ die Anzahl der verschiedenen Primteiler, $\Omega(n)$ die Anzahl der Primfaktoren und $\log n$ der natürliche Logarithmus von $n \in \mathbb{N}$. Dann gilt $\omega, \Omega, \log \in \mathcal{A}$, insbesondere sind Ω, log und die Nullfunktion 0 mit $0(n) = 0$ für alle $n \in \mathbb{N}$ sogar vollständig additiv.

Beispiel 2. Es sei $\tau(n)$ die Anzahl der natürlichen Teiler, $\sigma(n)$ die Summe der natürlichen Teiler von $n \in \mathbb{N}$ und $\varphi(n)$ die Anzahl der primen Restklassen mod n. Dann gilt $\tau, \sigma, \varphi \in \mathcal{M}$. Mit $\alpha \in \mathbb{R}$ sei $I^\alpha \in \mathcal{F}$ erklärt durch $I^\alpha(n) = n^\alpha$ für alle $n \in \mathbb{N}$. Dann sind I^α, $1 = I^0$, $I = I^1$, $\varepsilon \in \mathcal{M}$ sogar vollständig multiplikativ.

Folgerung 3. Additive und multiplikative Funktionen besitzen folgende Eigenschaften.

a) Jedes $f \in \mathcal{A} \cup \mathcal{M}$ ist durch die Werte $f(p^\nu)$ auf der Menge $\mathbb{P}^* = \{p^\nu : p \in \mathbb{P}, \nu \in \mathbb{N}\}$ der Primzahlpotenzen schon eindeutig bestimmt. Ist f vollständig additiv oder vollständig multiplikativ, so ist f schon durch die Werte $f(p)$ auf $\mathbb{P}$ festgelegt.

b) Es gilt $f \in \mathcal{M}$ genau dann, wenn $f \neq 0$ und (2) gilt, und dieses ist wieder genau dann der Fall, wenn $f(1) = 1$ und (2) gilt.

c) Aus $f \in \mathcal{A}$ folgt $f(1) = 0$, und es gilt $e^f \in \mathcal{M}$.

Nachweis. a) Ist $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ mit paarweise verschiedenen $p_\varrho \in \mathbb{P}$ und $\nu_\varrho \in \mathbb{N}$ die kanonische Darstellung von $n \in \mathbb{N}$, so folgt

$$f(n) = \sum_{\varrho=1}^{r} f(p_\varrho^{\nu_\varrho}), \qquad \text{falls } f \in \mathcal{A},$$

$$f(n) = \prod_{\varrho=1}^{r} f(p_\varrho^{\nu_\varrho}), \qquad \text{falls } f \in \mathcal{M}.$$

Bei vollständig additiven bzw. vollständig multiplikativen Funtionen f gilt noch $f(p^\nu) = \nu f(p)$ bzw. $f(p^\nu) = f^\nu(p)$.

b) Aus $f \in \mathcal{M}$ folgt $f \neq 0$ und aus $f(n) \neq 0$ für ein $n \in \mathbb{N}$ weiter $\big(f(1) - 1\big) f(n) = 0$, also

$f(1) = 1$.

c) Aus $f \in \mathcal{A}$ kommt $f(1) = f(1) + f(1)$ und daraus $f(1) = 0$. Für teilerfremde $m, n \in \mathbb{N}$ folgt

$$(e^f)(mn) = e^{f(mn)} = e^{f(m)+f(n)} = e^{f(m)}\, e^{f(n)} = (e^f)(m)\,(e^f)(n),$$

wie behauptet. □

Satz 3. Die Klasse $\mathcal{A}$ ist Unterraum von $\mathcal{F}$ bezüglich der linearen Operationen. Die Klasse $\mathcal{M}$ ist Untergruppe von $\mathcal{F}^*$ bezüglich der Dirichletschen Faltung.

Beweis. Die Aussage über $\mathcal{A}$ ist trivial. Wegen Satz 2 bleibt zu zeigen, daß $\mathcal{M}$ unter der Faltung abgeschlossen ist und daß mit f auch f^{-1} in $\mathcal{M}$ liegt.

a) Für teilerfremde $m, n \in \mathbb{N}$ hat jeder Teiler $d \in \mathbb{N}$ von mn eine eindeutige Darstellung der Form $d = ab$ mit $a, b \in \mathbb{N}$, $a \mid n$ und $b \mid m$. Es gelten $(a, b) = 1$, $\left(\frac{m}{a}, \frac{n}{b}\right) = 1$. Damit folgt für $f, g \in \mathcal{M}$

$$\begin{aligned}(f * g)(mn) &= \sum_{d \mid mn} f(d)\, g\Big(\frac{mn}{d}\Big) = \sum_{a \mid m, b \mid n} f(ab)\, g\Big(\frac{m}{a}\frac{n}{b}\Big) \\ &= \sum_{a \mid m} f(a)\, g\Big(\frac{m}{a}\Big) \sum_{b \mid n} f(b)\, g\Big(\frac{n}{a}\Big) = (f * g)(m)\,(f * g)(n).\end{aligned}$$

b) Zu $f \in \mathcal{M}$ existiert $f^{-1} \in \mathcal{F}^*$. Damit definieren wir eine multiplikative Funktion $g \in \mathcal{M}$ durch

$$g(p^\nu) = f^{-1}(p^\nu) \qquad (p^\nu \in \mathbb{P}^*)$$

und multiplikative Fortsetzung auf $\mathbb{N}$. Dann ist gemäß a) auch $f * g \in \mathcal{M}$, und für $p^\nu \in \mathbb{P}^*$ gilt

$$(f * g)(p^\nu) = \sum_{d \mid p^\nu} f(d)\, g\Big(\frac{p^\nu}{d}\Big) = \sum_{d \mid p^\nu} f(d)\, f^{-1}\Big(\frac{p^\nu}{d}\Big) = \varepsilon(p^\nu).$$

Es folgt $f * g = \varepsilon$ auf $\mathbb{P}^*$ und, da beide Seiten dieser Gleichung multiplikative Funktionen sind, $f * g = \varepsilon$ auf $\mathbb{N}$, also $f^{-1} = g \in \mathcal{M}$. □

Folgerung 4. Aus $h = f * g \in \mathcal{M}$ folgt $f, g \in \mathcal{M}$ oder $f, g \notin \mathcal{M}$.

Nachweis. Aus $h \in \mathcal{M}$ und etwa $f \in \mathcal{M}$ kommt mit Satz 3 sofort $g = h * f^{-1} \in \mathcal{M}$. □

Es ist offensichtlich, daß $\mathcal{A}$ die multiplikative Struktur von $\mathcal{F}$ nicht aufweist und daß bei $\mathcal{M}$ die lineare Struktur von $\mathcal{F}$ verloren geht.

7.3 Beispiele und Anwendungen

Definition. Es sei $\alpha \in \mathbb{R}$ und $1 < k \in \mathbb{N}$. Die Teilersummenfunktionen σ^α, die Teilerfunktionen τ_k und die Möbiusfunktion μ (Möbius, 1790 - 1868) sind erklärt durch

$$\begin{aligned} \sigma^\alpha &= 1 * I^\alpha, \\ \tau_k &= 1 * \cdots * 1 \qquad \text{mit } k \text{ Faktoren } 1, \\ \mu &= 1^{-1}. \end{aligned}$$

Folgerung 5. Die oben erklärten Funktionen sind alle multiplikativ. Speziell gilt $\tau_2 = \tau$, $\sigma_1 = \sigma$ sowie

$$\tau(n) = \sum_{d|n} 1 = \prod_{p^\nu \| n} (\nu + 1);$$

$$\sigma(n) = \sum_{d|n} d = \prod_{p^\nu \| n} (1 + p + \cdots + p^\nu);$$

$$\mu(n) = \begin{cases} (-1)^r & \text{für } n = p_1 \cdots p_r \text{ mit paarweise verschiedenen } p_\varrho \in \mathbb{P} \\ 0 & \text{sonst.} \end{cases}$$

Nachweis. Die Funktionen sind als Faltungsprodukte oder Faltungsinverse multiplikativer Funktionen ebenfalls multiplikativ. Die Produktdarstellungen rechnet man mit $\tau(p^\nu) = \nu + 1$ und $\sigma(p^\nu) = 1 + p + p^2 + \cdots + p^\nu$ nach. Für die Möbiusfunktion folgt aus $1 * \mu = \varepsilon$ an den Primzahlpotenzstellen $p^\nu \in \mathbb{P}^*$ mit $\nu \geq 2$

$$\begin{aligned} (\mu * 1)(p) &= 1 + \mu(p) = 0, \\ (\mu * 1)(p^\nu) &= \sum_{d|p^\nu} \mu(d) = \big(1 + \mu(p)\big) + \mu(p^2) + \cdots + \mu(p^\nu) = 0, \end{aligned}$$

woraus die Behauptung über die Werte $\mu(p^\nu)$ kommt. □

Bemerkung 1. In den Folgerungen 1 und 2 wird oft vorausgesetzt, daß $h \in \mathcal{M}$ vollständig multiplikativ ist. Der Vorteil besteht darin, daß in diesem Fall $h^{-1} = \mu\, h$ gilt, denn

$$(\mu\, h * h)(n) = \sum_{dm=n} \mu(d)\, h(d)\, h(m) = h(n) \sum_{dm=n} \mu(d) = h(n)\, \varepsilon(n) = \varepsilon(n).$$

In diesem Spezialfall erhalten die Folgerungen ein etwas einfacheres Aussehen. Die Äquivalenz der resultierenden Gleichungen $f = g * h$ und $g = f * \mu\, h$ nennt man auch 1. Möbiussche Umkehrformel, und die entsprechende Äquivalenz aus Folgerung 2 wird 2. Möbiussche Umkehrformel genannt. Zumeist findet man den Fall $h = 1$, also $h^{-1} = \mu$.

Satz 4. Für die Eulerfunktion φ gilt $\varphi = \mu * I$.

Beweis. Die Gleichungen $\varphi = \mu * I$ und $\varphi * 1 = I$ sind äquivalent. Letztere besagt

$$\sum_{d|n} \varphi(d) = n \qquad \text{für alle } n \in \mathbb{N}.$$

Dies ist die Aussage von Satz 7 aus Kapitel 3. □

Folgerung 6. Es gilt

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d} = n \prod_{p|n} \Big(1 - \frac{1}{p}\Big) \qquad (n \in \mathbb{N}).$$

Nachweis. Die erste Gleichung kommt aus Satz 4. Die rechte Seite der zweiten Gleichung ist eine multiplikative Funktion von n. An Primzahlpotenzen $n = p^\nu \in \mathbb{P}^*$ stimmt sie offenbar mit $\varphi(n) = p^\nu - p^{\nu-1}$ überein. Also gilt die Gleichung schon für alle $n \in \mathbb{N}$. □

Satz 5. Es sei $f \in \mathcal{A}$. Dann gilt

$$(\mu * f)(n) = \begin{cases} f(p^\nu) - f(p^{\nu-1}) & \text{für } n = p^\nu \in \mathbb{P}^* \\ 0 & \text{sonst} \end{cases} \qquad (n \in \mathbb{N}).$$

Beweis. Da f additiv ist, gilt $(\mu * f)(1) = f(1) = 0$, und wegen $\mu(p^\varrho) = 0$ für alle $p \in \mathbb{P}$ und $\varrho > 1$ kommt $(\mu * f)(p^\nu) = f(p^\nu) - f(p^{\nu-1})$ für $p^\nu \in \mathbb{P}^*$. Hat schließlich $n \in \mathbb{N}$ die Gestalt $n = ab$ mit teilerfremden $a, b \in \mathbb{N}$, so hat jeder natürliche Teiler d von n die Gestalt $d = a'b'$ mit eindeutig bestimmten natürlichen $a' \mid a$ und $b' \mid b$. Damit folgt

$$\begin{aligned}(\mu * f)(n) &= \sum_{d|ab} \mu\Big(\frac{ab}{d}\Big) f(d) = \sum_{\substack{a'|a \\ b'|b}} \mu\Big(\frac{a}{a'}\Big)\mu\Big(\frac{b}{b'}\Big)\big(f(a') + f(b')\big) \\ &= (\mu * f)(a)\,\varepsilon(b) + (\mu * f)(b)\,\varepsilon(a).\end{aligned}$$

Dies verschwindet für $a > 1$ und $b > 1$. □

Eine in der Primzahltheorie wichtige Anwendung von Satz 5 geht auf von Mangoldt (1854 - 1925) zurück.

Definition. Die von Mangoldt-Funktion $\Lambda : \mathbb{N} \to \mathbb{R}$ ist erklärt durch $\Lambda = \mu * \log$.

Aus Satz 5 kommt sofort die

Folgerung 7. Es gilt

$$\Lambda(n) = \begin{cases} \log p & \text{für } n = p^\nu \in \mathbb{P}^* \\ 0 & \text{sonst} \end{cases} \qquad (n \in \mathbb{N}).$$

Kapitel 8

Elementare analytische Techniken

In diesem Kapitel werden elementare analytische Techniken zur Untersuchung des mittleren Verhaltens arithmetischer Funktionen bereitgestellt und angewandt.

8.1 Partielle Summation

Die Werte arithmetischer Funktionen sind oft sehr unregelmäßig verteilt. Die Teilerfunktion τ ist dafür ein typisches Beispiel; sie ist beliebig großer Werte fähig, nimmt aber den Funktionswert 2 unendlich oft an. Dagegen erweist sich das Verhalten der Summe

$$\sum_{n \le x} f(n)$$

häufig als ziemlich regelmäßig, und sie läßt sich durch bekannte reell- oder komplexwertige Funktionen gut approximieren. Ein wesentlicher Teil des Studiums arithmetischer Funktionen besteht in der Untersuchung ihres summatorischen Verhaltens. Ist insbesondere f die charakteristische Funktion einer Menge von natürlichen Zahlen, etwa der Primzahlmenge $\mathbb{P}$, so werden auch Abzählungsprobleme davon erfaßt.

Definition. Es sei $a \ge 0$ reell, $f \in \mathcal{F}$. Dann heißt die durch

$$s_f(x) = s_f(a,x) = \sum_{a < n \le x} f(n) \qquad (x \ge 0)$$

erklärte Treppenfunktion $s_f : [0,\infty) \to \mathbb{C}$ eine summatorische Funktion von f.

Bemerkung 1. Die Funktion s_f ist rechtsseitig stetig. Es gilt $s_f(a,x) = 0$ für $x < 1$ oder $x \le a$. Für $0 \le a \le b \le x$ gilt $s_f(a,x) = s_f(a,b) + s_f(b,x)$.

Völlig abweichend von unserer an die Limitierungstheorie angelehnten Definition findet man bisweilen in der Literatur auch das Dirichletsche Faltungsprodukt $1 * f$ als summatorische Funktion von f bezeichnet.

Beispiel 1. Es gilt $s_1(0,x) = [x]$, $s_I(0,x) = \frac{1}{2}\,[x]\big([x]+1\big)$.

Ein wesentliches technisches Hilfsmittel zur Berechnung von Integralen ist das Verfahren der partiellen Integration. Unter geeigneten Differenzierbarkeitsvoraussetzungen an die Funktionen f, g besteht

$$\int_a^x f(t)\,g(t)\,dt = F(x)\,g(x) - \int_a^x F(t)\,g'(t)\,dt\,,$$

wobei F Stammfunktion von f mit $F(a) = 0$ ist. Das analoge Hilfsmittel zur Berechnung von Summen geht auf Abel (1802 - 1829) zurück; es handelt sich um das Verfahren der (abelschen) partiellen Summation.

Satz 1. Es sei $0 \le a \le x$, $f \in \mathcal{F}$ und $g : [a,x] \to \mathbb{C}$ eine stetige und stückweise stetig differenzierbare Funktion. Dann gilt

$$s_{fg}(a,x) = s_f(a,x)g(x) - \int_a^x s_f(a,t)\,g'(t)\,dt.$$

Beweis. Man rechnet nach

$$\begin{aligned}
s_{fg}(a,x) &= \sum_{a<n\le x} f(n)\,g(n) = \sum_{a<n\le x} \big(s_f(a,n) - s_f(a,n-1)\big)\,g(n)\\
&= \sum_{a<n\le x} s_f(a,n)\,g(n) - \sum_{a<n\le x-1} s_f(a,n)\,g(n+1)\\
&= s_f(a,x)\,g([x]) - \sum_{a<n\le x-1} s_f(a,n)\,\big(g(n+1) - g(n)\big)\\
&= s_f(a,x)\,g([x]) - \sum_{a<n\le x-1} s_f(a,n) \int_n^{n-1} g'(t)\,dt\\
&= s_f(a,x)\,g([x]) - \int_a^{[x]} s_f(a,t)\,g'(t)\,dt\\
&= s_f(a,x)\,g(x) - \int_a^x s_f(a,t)\,g'(t)\,dt\,,
\end{aligned}$$

wobei zuletzt

$$s_f(a,x)\,(g(x) - g([x])) = \int_{[x]}^x s_f(a,t)\,g'(t)\,dt$$

verwendet wurde. □

Folgerung 1. Es bezeichne $B_1 : \mathbb{R} \to \mathbb{R}$ die durch

$$B_1(t) = t - \frac{1}{2} \quad \text{für } 0 \le t < 1$$

und 1-periodische Fortsetzung auf $\mathbb{R}$ definierte Bernoulli-Funktion (Jakob Bernoulli, 1654 - 1705). Es sei weiter $0 \le a \le x$ und $g : [a,x] \to \mathbb{C}$ stetig und stückweise stetig differenzierbar.

Dann gilt

$$s_g(a,x) = \int_a^x g(t)\,dt - B_1(t)\,g(t)\Big|_a^x - \int_a^x B_1(t)\,g'(t)\,dt\,. \tag{1}$$

Nachweis. Mit $f = 1$ und $s_f(a,x) = [x] - [a]$ kommt

$$\begin{aligned} s_g(a,x) &= \big([x]-[a]\big)\,g(x) - \int_a^x \big([t]-[a]\big)\,g'(t)\,dt \\ &= [x]\,g(x) - [a]\,g(a) - \int_a^x \Big(t - \frac{1}{2}\Big)\,g'(t)\,dt + \int_a^x \Big(t-[t]-\frac{1}{2}\Big)\,g'(t)\,dt \\ &= \int_a^x g(t)\,dt - \Big(t-[t]-\frac{1}{2}\Big)\,g(t)\Big|_a^x + \int_a^x \Big(t-[t]-\frac{1}{2}\Big)\,g'(t)\,dt \\ &= \int_a^x g(t)\,dt - B_1(t)\,g(t)\Big|_a^x + \int_a^x B_1(t)\,g'(t)\,dt \end{aligned}$$

□

Bemerkung 2. Formel (1) ist ein Spezialfall der sogenannten Eulerschen Summenformel. Diese entsteht aus (1) durch weitere partielle Summation des letzten Integrals, wobei g als genügend oft differenzierbar vorauszusetzen ist. Als sukzessive Stammfunktionen treten dabei die 1-periodischen Bernoulli-Funktionen B_k auf mit

$$B_{k+1}(x) = (k+1)\Big(\int_0^x B_k(t)\,dt + \int_0^1 tB_k(t)\,dt\Big) \qquad (k \in \mathbb{N},\ 0 \le x < 1)$$

Die B_k sind für $k \ge 2$ auf $\mathbb{R}$ stetig, und sie haben die Mittelwerteigenschaft

$$\int_0^1 B_k(t)\,dt = 0 \qquad (k \in \mathbb{N}).$$

Die sogenannten Bernoullischen Zahlen sind die Werte $B_k(0)$. Man rechnet etwa nach $B_2(x) = x^2 - x + \frac{1}{6}$ für $0 \le x < 1$. Von Interesse sind die Fourierentwicklungen, etwa

$$B_2(x) = \frac{1}{\pi^2}\sum_{n=1}^{\infty} \frac{\cos(2\pi nx)}{n^2} \qquad (x \in \mathbb{R}).$$

Damit folgt $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$.

8.2 Die Landauschen Symbole

Bevor wir Satz 1 und Folgerung 1 anwenden, führen wir eine zweckmäßige Schreibweise ein, die auf Landau (1877 - 1938) zurückgeht.

Definition. Es sei $M \subseteq \mathbb{C}$, $a \in \mathbb{C} \cup \{\infty\}$ ein Häufungspunkt von M, ferner $f, g : M \to \mathbb{C}$ und $r : M \to \mathbb{R}_+$. Man schreibt mit den Landauschen Symbolen $\mathcal{O}$ und o

$$f(z) = g(z) + \mathcal{O}(r(z)) \text{ für } z \in M \quad \text{anstelle von} \quad \bigvee_{c \in \mathbb{R}_+} \bigwedge_{z \in M} \frac{|f(z) - g(z)|}{r(z)} \leq c,$$

$$f(z) = g(z) + o(r(z)) \text{ für } z \to a \quad \text{anstelle von} \quad \lim_{\substack{z \to a \\ z \in M}} \frac{f(z) - g(z)}{r(z)} = 0.$$

Asymptotische Gleichheit ist erklärt durch

$$f(z) \sim g(z) \text{ für } z \to a \quad \text{genau dann, wenn} \quad \lim_{\substack{z \to a \\ z \in M}} \frac{f(z)}{g(z)} = 1.$$

Anstelle des Landauschen $\mathcal{O}$ Symbols ist auch das von Vinogradov (1891 - 1983) eingeführte Symbol $\ll$ gebräuchlich: Es bedeutet $f(z) \ll r(z)$ dasselbe wie $f(z) = \mathcal{O}\big(r(z)\big)$.

Bemerkung 3. Genau dann besteht $f(z) \sim g(z)$ für $z \to a$, wenn $f(z) = g(z) + o(|g(z)|)$ für $z \to a$ gilt.

Es sei $M = \mathbb{N}$, $a = \infty$ und $f \in \mathcal{F}$. Dann bedeutet $f(n) = o(1)$, daß f eine Nullfolge ist, und $f(n) = \mathcal{O}(1)$, daß f eine beschränkte Folge ist. Die Tatsache, daß jede Nullfolge beschränkt ist, drückt die „Gleichung“ $o(1) = \mathcal{O}(1)$ aus. Es ist offensichtlich, daß die Verwendung des Gleichheitszeichens im Zusammenhang mit den Landauschen Symbolen logisch nicht einwandfrei ist. Mit der Element- und der Inklusionsbeziehung wäre aber solchen Einwänden leicht der Boden zu entziehen. In der Tat führen die (eingebürgerten) Landauschen Symbole zu einer so großen Vereinfachung der Schreibweise und des Verständnisses, daß puristische Kleinlichkeit unangebracht ist.

Beispiel 2. Der ersten Orientierung dienen die folgenden Abschätzugen: $\sin x = \mathcal{O}(1)$ für $x \in \mathbb{R}$, $[x] = x + \mathcal{O}(1)$ für $x \in \mathbb{R}$, $\sin x = x + \mathcal{O}(|x|^3)$ für $x \to 0$, $\log(1+x) \sim x$ für $x \to 0$, $\log x = \mathcal{O}(x^\varepsilon)$ für $x \geq 1$ und jedes $\varepsilon > 0$, $e^x = 1 + \mathcal{O}(|x|)$ für $|x| \leq 1$, $\exp\big(o(1)\big) = 1 + o(1)$ für $x \to a$, $x \sim x + 1$ für $x \to \infty$, $\log x \sim \log(x+1)$ für $x \to \infty$, $e^x \not\sim e^{x+1}$ für $x \to \infty$.

8.3 Elementare asymptotische Formeln

Wir untersuchen das asymptotische Verhalten einiger spezieller Summen, die oft benötigt werden.

Satz 2. Es sei $x \geq 1$. Dann gilt

$$\sum_{n \leq x} \frac{1}{n^\alpha} = \begin{cases} \log x + \gamma + \mathcal{O}\Big(\dfrac{1}{x}\Big) & \text{für } \alpha = 1 \\ \dfrac{x^{1-\alpha}}{1-\alpha} + \gamma_\alpha + \mathcal{O}\Big(\dfrac{1}{x^\alpha}\Big) & \text{für } 0 < \alpha < 1. \end{cases}$$

Dabei sind γ, γ_α Konstanten mit den Darstellungen $(0 < \alpha < 1)$

$$\gamma = \frac{1}{2} - \int_1^\infty \frac{B_1(t)}{t^2}\, dt, \quad \gamma_\alpha = \frac{1}{2} - \frac{1}{1-\alpha} - \alpha \int_1^\infty \frac{B_1(t)}{t^{1+\alpha}}\, dt.$$

Beweis. Für $\alpha = 1$ liefert Folgerung 1 mit $0 < \delta < 1$

$$\begin{aligned}\sum_{n\le x}\frac{1}{n} &= \int_{1-\delta}^{x}\frac{dt}{t} + \frac{B_1(1-\delta)}{1-\delta} - \frac{B_1(x)}{x} - \int_{1-\delta}^{x}\frac{B_1(t)}{t^2}\,dt \\ &= \int_{1-\delta}^{x}\frac{dt}{t} + \frac{B_1(1-\delta)}{1-\delta} - \frac{B_1(x)}{x} - \int_{1-\delta}^{\infty}\frac{B_1(t)}{t^2}\,dt + \int_{x}^{\infty}\frac{B_1(t)}{t^2}\,dt\,,\end{aligned}$$

also für $\delta \to 0+$ bereits

$$\sum_{n\le x}\frac{1}{n} = \log x + \gamma + R(x)$$

mit

$$|R(x)| \le \frac{|B_1(x)|}{x} + \int_{x}^{\infty}\frac{|B_1(t)|}{t^2}\,dt \le \frac{1}{x} = \mathcal{O}\Big(\frac{1}{x}\Big).$$

Die Behauptung im Fall $0 < \alpha < 1$ ergibt sich entsprechend unter Beachtung der absoluten Konvergenz des Integrals

$$\alpha\int_{x}^{\infty}\frac{B_1(t)}{t^{1+\alpha}}\,dt \ll \frac{1}{x^{\alpha}} \qquad (x \ge 1).$$

□

Bemerkung 4. Es ist γ die bekannte Euler-Mascheroni-Konstante,

$$\gamma = \lim_{x\to\infty}\Big(\sum_{n\le x}\frac{1}{n} - \log x\Big).$$

Satz 3. Mit der Konstanten $c = 1 + \displaystyle\int_{1}^{\infty}\frac{B_1(t)}{t}\,dt$ gilt für $n \in \mathbb{N}$

$$\sum_{\nu\le n}\log\nu = n\log n - n + \frac{1}{2}\log n + c + \mathcal{O}\Big(\frac{1}{n}\Big).$$

Beweis. Wir zeigen zuerst die Existenz von

$$\int_{n}^{\infty}\frac{B_1(t)}{t}\,dt \ll \frac{1}{n}\,.$$

Für $k \in \mathbb{N}$ liefert die Substitution $u = t - k - \frac{1}{2}$

$$\int_{k}^{k+1}\frac{B_1(t)}{t}\,dt = \int_{-\frac{1}{2}}^{\frac{1}{2}}\frac{u\,du}{u+k+\frac{1}{2}} = -\int_{0}^{\frac{1}{2}}\frac{2u^2}{\big(k+\frac{1}{2}\big)^2 - u^2}\,du\,,$$

also

$$0 \le -\int_{k}^{k+1}\frac{B_1(t)}{t}\,dt \le \frac{1}{4k^2}\,,$$

woraus die behauptete Konvergenz und die Abschätzung

$$\Big|\int_{n}^{\infty}\frac{B_1(t)}{t}\,dt\Big| \le \frac{1}{4}\sum_{k=n}^{\infty}\frac{1}{k^2} \ll \frac{1}{n}$$

ablesbar sind. Nun ergibt Folgerung 1

$$\sum_{\nu\le n}\log\nu=\int_1^n\log t\,dt-B_1(t)\,\log t\Big|_1^n+\int_1^n\frac{B_1(t)}{t}\,dt$$
$$=n\log n-n+1+\frac12\log n+\int_1^\infty\frac{B_1(t)}{t}\,dt+\mathcal{O}\Big(\frac1n\Big).$$

□

Bemerkung 5. Aus der Grundvorlesung über Analysis ist $c=\frac12\log 2\pi$ bekannt; Satz 3 ist nämlich die logarithmische Version der Stirlingschen Formel $n!\sim\sqrt{2\pi n}\left(\frac ne\right)^n$ für $n\to\infty$ mit dem genaueren Restglied $\mathcal{O}\big(\frac1n\big)$ statt $o(1)$.

8.4 Die mittlere Größenordnung einiger arithmetischer Funktionen

Hier behandeln wir die summatorischen Funktionen von σ,φ,τ und beweisen zur Vorbereitung den folgenden

Satz 4. Es bestehen die folgenden Konvergenzaussagen:

a) Konvergieren beide Reihen $\sum f(n)$ und $\sum g(n)$ mit $f,g\in\mathcal{F}$ absolut, so konvergiert auch die Reihe $\sum(f*g)(n)$ absolut, und es gilt

$$\sum_{n=1}^\infty(f*g)(n)=\sum_{n=1}^\infty f(n)\,\sum_{n=1}^\infty g(n)\,.$$

b) Es sei $f\in\mathcal{M}$. Genau dann konvergiert die Absolutreihe $\sum|f(n)|$, wenn das Absolutprodukt $\prod\limits_{p\in\mathbb{P}}\big(1+|f(p)|+|f(p^2)|+\cdots\big)$ konvergiert, und in diesem Falle gilt die Eulersche Produktformel

$$\sum_{n=1}^\infty f(n)=\prod_{p\in\mathbb{P}}\big(1+f(p)+f(p^2)+\cdots\big).$$

Im Fall der vollständigen Multiplikativität von f gilt dann sogar

$$\sum_{n=1}^\infty f(n)=\prod_{p\in\mathbb{P}}\big(1-f(p)\big)^{-1}.$$

Beweis. a) Die Reihen dürfen ausmultipliziert und umgeordnet werden. Bei geeigneter Zusammenfassung der Glieder entsteht

$$\sum_{m=1}^\infty f(m)\sum_{d=1}^\infty g(d)=\sum_{m,d=1}^\infty f(m)\,g(d)=\sum_{n=1}^\infty\sum_{md=n}f(m)\,g(d)=\sum_{n=1}^\infty(f*g)(n)\,,$$

und die Produktreihe konvergiert absolut.

b) Aus der Konvergenz des Absolutprodukts und der Ungleichung

$$\sum_{n\le N} |f(n)| \le \prod_{\substack{p\le N\\ p\in\mathbb{P}}} \big(1+|f(p)|+|f(p^2)|+\cdots\big) \le \prod_{p\in\mathbb{P}} \big(1+|f(p)|+|f(p^2)|+\cdots\big) < \infty$$

kommt die Konvergenz von $\sum\limits_{n=1}^{\infty} |f(n)|$. Umgekehrt kommt aus der Konvergenz der Absolutreihe die von $1+|f(p)|+|f(p^2)|+\cdots$ für jedes $p\in\mathbb{P}$, und die Abschätzung

$$\begin{aligned}\Big|\prod_{p\le N}\big(1+f(p)+f(p^2)+\cdots\big) - \sum_{n\le N} f(n)\Big| &= \Big|\sum_{\substack{n>N\\ p|n\Rightarrow p\le N}} f(n)\Big| \\ &\le \sum_{\substack{n>N\\ p|n\Rightarrow p\le N}} |f(n)| = \prod_{p\le N}\big(1+|f(p)|+|f(p^2)|+\cdots\big) - \sum_{n\le N}|f(n)| \\ &\le \sum_{n>N}|f(n)| = \mathcal{O}(1) \quad \text{für } n\to\infty\end{aligned}$$

liefert die Konvergenz des Absolutprodukts und die behauptete Produktformel. Der Zusatz für vollständig multiplikatives f folgt daraus durch Summation der geometrischen Reihen

$$1+f(p)+f(p^2)+\cdots = 1+f(p)+f^2(p)+\cdots = \frac{1}{1-f(p)}\,.$$

□

Definition. Die Riemannsche Zetafunktion ist für $s>1$ definiert durch

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

Folgerung 2. Die Zeta-Reihe konvergiert absolut für alle $s>1$ und gleichmäßig für alle $s\ge 1+\varepsilon$ mit $\varepsilon>0$. Für $s>1$ ist $\zeta(s)$ stetig, und es gelten dort die absolut konvergenten Produktdarstellungen

$$\zeta(s) = \prod_{p\in\mathbb{P}} \Big(1-\frac{1}{p^s}\Big)^{-1}, \quad \frac{1}{\zeta(s)} = \sum_{n=1}^{\infty}\frac{\mu(n)}{n^s} = \prod_{p\in\mathbb{P}}\Big(1-\frac{1}{p^s}\Big)\,.$$

Insbesondere gilt $\zeta(2) = \dfrac{\pi^2}{6}$.

Nachweis. Die Behauptungen folgen aus Satz 4, wobei im Fall der Möbiusfunktion $1*\mu=\varepsilon$ sowie $|\mu(n)|\le 1$ für alle $n\in\mathbb{N}$ eingeht. Der Zusatz kommt aus Bemerkung 2. □

Satz 5. Für $x\ge 2$ gilt

a) $\displaystyle\sum_{n\le x}\sigma(n) = \frac{\zeta(2)}{2}\,x^2 + \mathcal{O}(x\log x)\,,$ b) $\displaystyle\sum_{n\le x}\varphi(n) = \frac{1}{2\zeta(2)}\,x^2 + \mathcal{O}(x\log x).$

Beweis. a) Wegen $\sigma = 1 * I$ liefern die Sätze 1 und 2 sowie Folgerung 2

$$\begin{aligned}\sum_{n\le x}\sigma(n) &= \sum_{n\le x}\sum_{d\mid n} d = \sum_{dm\le x} d = \sum_{m\le x}\sum_{d\le x/m} d = \frac{1}{2}\sum_{m\le x}\Big(\Big(\frac{x}{m}\Big)^2 + \mathcal{O}\Big(\frac{x}{m}\Big)\Big)\\ &= \frac{x^2}{2}\sum_{m=1}^{\infty}\frac{1}{m^2} + \mathcal{O}\bigg(x^2\sum_{m>x}\frac{1}{m^2}\bigg) + \mathcal{O}\bigg(x\sum_{m\le x}\frac{1}{m}\bigg)\\ &= \frac{\zeta(2)}{2}\,x^2 + \mathcal{O}\bigg(x^2\int_x^{\infty}\frac{dt}{t^2}\bigg) + \mathcal{O}\big(x\log x\big) = \frac{\zeta(2)}{2}\,x^2 + \mathcal{O}\big(x\log x\big).\end{aligned}$$

b) Mit $\varphi = \mu * I$ folgt analog

$$\begin{aligned}\sum_{n\le x}\varphi(n) &= \sum_{n\le x}\sum_{d\mid n}\mu(d)\,\frac{n}{d} = \sum_{dm\le x}\mu(d)\,m = \sum_{d\le x}\mu(d)\sum_{m\le x/d} m\\ &= \frac{1}{2}\sum_{d\le x}\mu(d)\,\Big(\Big(\frac{x}{d}\Big)^2 + \mathcal{O}\Big(\frac{x}{d}\Big)\Big) = \frac{x^2}{2}\sum_{d\le x}\frac{\mu(d)}{d^2} + \mathcal{O}\bigg(x\sum_{d\le x}\frac{1}{d}\bigg)\\ &= \frac{x^2}{2}\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2} + \mathcal{O}\bigg(x^2\sum_{d>x}\frac{1}{d^2}\bigg) + \mathcal{O}\big(x\log x\big) = \frac{x^2}{2\zeta(2)} + \mathcal{O}(x\log x).\end{aligned}$$

□

Satz 6. Für $x \ge 1$ gilt $\displaystyle\sum_{n\le x}\tau(n) = x\log x + (2\gamma-1)x + \mathcal{O}\big(\sqrt{x}\big)$.

Beweis. Mit $\tau * \tau = 1$ kommt aus Satz 2 zunächst

$$\begin{aligned}\sum_{n\le x}\tau(n) &= \sum_{n\le x}\sum_{md=n} 1 = \sum_{md\le x} 1 = \sum_{m\le x}\sum_{d\le x/m} 1 = \sum_{m\le x}\Big[\frac{x}{m}\Big]\\ &= \sum_{m\le x}\Big(\frac{x}{m} + \mathcal{O}(1)\Big) = x\sum_{m\le x}\frac{1}{m} + \mathcal{O}(x) = x\log x + \mathcal{O}(x),\end{aligned}$$

was zum Beweis der Behauptung offenbar nicht ausreicht. Zur Verbesserung der Abschätzung folgen wir Gauß und gehen auf

$$\sum_{n\le x}\tau(n) = \sum_{dm\le x} 1$$

zurück. Rechts steht die Anzahl der Gitterpunkte $(d,m) \in \mathbb{N}^2$, die im ersten Quadranten unterhalb oder auf der Hyperbel $dm = x$ liegen. Aus Symmetriegründen folgt mit Satz 2

$$\begin{aligned}\sum_{n\le x}\tau(n) &= \sum_{md\le x} 1 = 2\sum_{m\le\sqrt{x}}\sum_{d\le\frac{x}{m}} 1 - \big[\sqrt{x}\big]^2\\ &= 2\sum_{m\le\sqrt{x}}\Big(\frac{x}{m} + \mathcal{O}(1)\Big) - x + \mathcal{O}\big(\sqrt{x}\big) = 2x\sum_{m\le\sqrt{x}}\frac{1}{m} - x + \mathcal{O}\big(\sqrt{x}\big)\\ &= 2x\,\Big(\log\sqrt{x} + \gamma + \mathcal{O}\Big(\frac{1}{\sqrt{x}}\Big)\Big) - x + \mathcal{O}\big(\sqrt{x}\big)\\ &= x\log x + (2\gamma-1)x + \mathcal{O}\big(\sqrt{x}\big),\end{aligned}$$

wie behauptet. □

Bemerkung 6. Man kann fragen, für welche Exponenten ϑ die Aussage

$$\sum_{n\le x} \tau(n) = x\log x + (2\gamma - 1)x + \mathcal{O}\Big(x^{\vartheta}\Big)$$

zutrifft. Es sei $\lambda = \inf \vartheta$. Die Bestimmung von λ ist das sogenannte Dirichletsche Teilerproblem. Man weiß etwa

$$\frac{1}{4} \le \lambda \le \frac{35}{108}$$

(man beachte $\frac{35}{108} < \frac{1}{3}$). Die untere Schranke stammt von Hardy und Landau (1915), die obere geht zurück auf Kolesnik (1982). Die Schranke $\frac{1}{3}$ wurde schon 1903 von Voronoi bestimmt. Es gibt weitere Verbesserungen der oberen Schranke. Man vermutet $\lambda = \frac{1}{4}$.

Bemerkung 7. Durch partielle Summation lassen sich aus den Sätzen 5 und 6 asymptotische Aussagen für die Summen

$$\sum_{n\le x} \frac{\sigma(n)}{n}, \quad \sum_{n\le x} \frac{\varphi(n)}{n}, \quad \sum_{n\le x} \frac{\tau(n)}{n}$$

mittels partieller Summation gewinnen. Etwa liefert Satz 1 für $x \ge 2$

$$\begin{aligned}\sum_{n\le x} \frac{\sigma(n)}{n} &= \frac{1}{x}\sum_{n\le x}\sigma(n) + \int_1^x \frac{1}{t^2}\sum_{n\le t}\sigma(n)\,dt \\ &= \zeta(2)\,x + \mathcal{O}\big(\log^2 x\big).\end{aligned}$$

Dabei wurde zuletzt $\displaystyle\int_1^x \frac{\log t}{t}\,dt = \frac{1}{2}\log^2 x$ verwendet.

Kapitel 9

Elementare Ergebnisse zur Primzahlverteilung

In diesem Kapitel werden die Verteilung der Primzahlen studiert und quantitative Ergebnisse mit elementaren Methoden bewiesen.

9.1 Die Abschätzungen von Chebyshev

Die Idee, aus der Primfaktorzerlegung von $n!$ quantitative Abschätzungen über die Anzahl der Primzahlen $p \leq x$ zu gewinnen, geht auf Chebyshev (1821 - 1894) zurück.

Definition. Für $x \geq 1$ bezeichnet $\pi(x)$ die Anzahl der Primzahlen $\leq x$.

Satz 1. Für $n \in \mathbb{N}$ gilt $n! = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}$ mit $\nu_p(n) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$.

Beweis. Produkt und Reihe sind jeweils endlich wegen $\left[\frac{n}{p^k}\right] = 0$ für $p^k > n$. Insbesondere läuft bei festem p die Summe $\nu_p(n)$ nur über die $k \in \mathbb{N}$ mit $k \leq \frac{\log n}{\log p}$, und das Produkt braucht nur über die Primzahlen $p \leq n$ erstreckt zu werden. Wir zählen ab, wie oft eine Primzahl $p \leq n$ in $n!$ aufgeht: Unter den Faktoren $1, 2, \ldots, n$ von $n!$ haben genau die Zahlen

$$\begin{aligned} &\lambda p && \text{mit } \lambda = 1, \ldots, \left[\frac{n}{p}\right] && \text{den Teiler } p, \\ &\lambda p^2 && \text{mit } \lambda = 1, \ldots, \left[\frac{n}{p^2}\right] && \text{den Teiler } p^2 \\ &\text{usw.} \end{aligned}$$

Der Gesamtbeitrag $\nu_p(n)$ der Primzahl p zu $n!$ ist daher $[\frac{n}{p}] + [\frac{n}{p^2}] + \cdots$, wie behauptet. □

Satz 2. Für $x \geq 2$ gilt die Abschätzung von Chebyshev

$$\frac{1}{4}\,\frac{x}{\log x} < \pi(x) < 4\,\frac{x}{\log x}\,.$$

Beweis. Wir betrachten für $n \in \mathbb{N}$ den Binomialkoeffizienten $\binom{2n}{n} \in \mathbb{N}$. Offenbar gilt

$$\prod_{n<p\leq 2n} p \leq \frac{(2n)!}{n!\,n!} = \binom{2n}{n} \leq 2^{2n},$$

also

$$\sum_{n<p\leq 2n} \log p \leq (2\log 2)\,n. \tag{1}$$

Es folgt $\pi(2n) \leq \pi(n) + 2\log 2\,\dfrac{n}{\log n}$ für alle $n \in \mathbb{N}$, $n \geq 2$. Es sei nun $x > 4$ mit $2^{k-1} < x \leq 2^k$ und $3 \leq k \in \mathbb{N}$. Wir machen die rekursive Ungleichung explizit:

$$\pi(x) \leq \pi(2^k) < \frac{2^k}{k-1} + \frac{2^{k-1}}{k-2} + \cdots + \frac{2^2}{1} + \pi(2) = 1 + 2\sum_{\nu=1}^{k-1} \frac{2^\nu}{\nu}\,.$$

Induktion nach k für $k \geq 3$ zeigt

$$1 + 2\sum_{\nu=1}^{k-1} \frac{2^\nu}{\nu} \leq \frac{2^{k+1}}{(k-1)\log 2} = 4\,\frac{2^{k-1}}{\log 2^{k-1}} < 4\,\frac{x}{\log x}\,.$$

Damit ist die beauptete Abschätzung von $\pi(x)$ nach oben für $x \geq 4$ gezeigt, und für $2 \leq x \leq 4$ verifiziert man sie direkt.

Andererseits liefern Induktion und Satz 1

$$2^n \leq \binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \prod_{p\leq 2n} p^{\nu_p(2n) - 2\nu_p(n)}. \tag{2}$$

Wegen

$$[2x] - 2[x] = \begin{cases} 0 & \text{für } 0 \leq \vartheta < \frac{1}{2} \\ 1 & \text{für } \frac{1}{2} \leq \vartheta < 1 \end{cases} \qquad (x = [x] + \vartheta)$$

folgt

$$\nu_p(2n) - 2\nu_p(n) = \sum_{k=1}^{\infty} \left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right] \right) \leq \frac{\log 2n}{\log p}\,.$$

Einsetzen in (2) liefert

$$2^n \leq \prod_{p\leq 2n} p^{\frac{\log 2n}{\log p}} = (2n)^{\pi(2n)},$$

und durch Logarithmieren entsteht $\pi(2n) \geq \frac{\log 2}{2} \frac{2n}{\log 2n}$ für $n \in \mathbb{N}$. Schachtelt man $x > 6$ ein durch $2n < x \leq 2n+2$ mit $n \in \mathbb{N}$, $n \geq 3$, so kommt

$$\begin{aligned}\pi(x) \geq \pi(2n) &\geq \left(\tfrac{\log 2}{2} \tfrac{2n}{x} \tfrac{\log x}{\log 2n}\right) \frac{x}{\log x} \\ &\geq \left(\tfrac{\log 2}{2} \tfrac{2n}{2n+2}\right) \frac{x}{\log x} \geq \left(\tfrac{3}{8} \log 2\right) \frac{x}{\log x} > \frac{1}{4} \frac{x}{\log x},\end{aligned}$$

und für $2 \leq x \leq 6$ verifiziert man dies wieder direkt. Damit ist die Abschätzung von Chebyshev vollständig nachgewiesen. □

Bemerkung 1. Satz 2 sagt aus, daß $\pi(x)$ die Größenordnung $\frac{x}{\log x}$ hat. Es gilt nämlich

$$\frac{1}{4} \leq \underline{\lim} \frac{\pi(x) \log x}{x} \leq \overline{\lim} \frac{\pi(x) \log x}{x} \leq 4.$$

9.2 Die Funktionen ϑ und ψ

Es ist zweckmäßig, anstelle von $\pi(x)$ die gewichteten Summen $\vartheta(x)$ und $\psi(x)$ zu untersuchen:

Definition. Für $x \geq 1$ sind ϑ, ψ erklärt durch

$$\vartheta(x) = \sum_{p \leq x} \log p, \quad \psi(x) = \sum_{p^\nu \leq x} \log p.$$

Bemerkung 2. Offenbar ist ψ die summatorische Funktion der von Mangoldt-Funktion Λ,

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

Folgerung 1. Für $x \geq 2$ gelten die Abschätzungen

$$\vartheta(x) - \pi(x) \log x \ll \frac{x}{\log x}, \quad \psi(x) - \vartheta(x) \ll \sqrt{x}.$$

Insbesondere gilt $\pi(x) \log x \sim \vartheta(x) \sim \psi(x)$ für $x \to \infty$.

Nachweis. Partielle Summation ergibt

$$\vartheta(x) = \sum_{p \leq x} \log p = \pi(x) \log x - \int_1^x \frac{\pi(t)}{t}\, dt.$$

Mit Satz 2 folgt

$$\int_1^x \frac{\pi(t)}{t}\, dt \leq 4 \int_2^x \frac{dt}{\log t} \ll \left(\int_2^{\sqrt{x}} + \int_{\sqrt{x}}^x\right) \frac{dt}{\log t} \ll \sqrt{x} + \frac{x}{\log x} \ll \frac{x}{\log x} \ll \pi(x).$$

Die zweite Abschätzung ergibt sich aus

$$\psi(x) - \vartheta(x) = \sum_{\substack{p^\nu \le x \\ \nu \ge 2}} \log p = \vartheta\big(\sqrt{x}\big) + \vartheta\big(\sqrt[3]{x}\big) + \cdots ,$$

wobei rechts wegen $\vartheta(y) = 0$ für $y < 2$ die Anzahl der nicht verschwindenden Summanden $\le \frac{\log x}{\log 2}$ ist. Aus Satz 2 und dem schon bewiesenen Teil von Folgerung 1 kommt $\vartheta(x) \ll x$ und damit

$$\psi(x) - \vartheta(x) \ll \sqrt{x} + \sqrt[3]{x}\,\log x \ll \sqrt{x}\,.$$

Wegen Satz 2 haben $\pi(x)\log x$, $\vartheta(x)$ und $\psi(x)$ die Größenordnung x. Die behauptete asymptotische Gleichheit folgt schließlich aus $\sqrt{x} = o(x)$ und $\pi(x) = o(x)$ für $x \to \infty$. □

Die Chebyshevschen Abschätzungen von $\pi(x)$ lassen sich auf $\vartheta(x)$ und $\psi(x)$ übertragen.

Folgerung 2. Es gibt eine Konstante $c > 0$, so daß gilt

$$cx \le \vartheta(x) < 3x\,, \quad cx \le \psi(x) < 4x \qquad (x \ge 2).$$

Nachweis. Es gilt

$$\psi(x) = \sum_{p^\nu \le x} \log p = \sum_{p \le x} \log p \sum_{1 \le \nu \le \frac{\log x}{\log p}} 1 \le \pi(x)\log x < 4x\,.$$

Zum Beweis von $\vartheta(x) < 3x$ gehen wir auf (1) zurück,

$$\vartheta(2n) - \vartheta(n) < (2\log 2)\,n \qquad (n \in \mathbb{N}).$$

Einschachteln von $x > 1$ durch Zweierpotenzen, $2^{k-1} < x \le 2^k$ mit $k \in \mathbb{N}$, ergibt

$$\vartheta(x) \le \vartheta(2^k) < \log 2\,\big(2^k + 2^{k-1} + \cdots + 2 + 1\big) < 2^{k+1}\log 2 < (4\log 2)\,x < 3x\,.$$

Wegen $\psi(x) \ge \vartheta(x)$ bleibt nur noch $\vartheta(x) \ge cx$ mit einer positiven Konstanten c für $x \ge 2$ zu zeigen. Aus Folgerung 1 und Satz 2 kommt

$$\vartheta(x) = \pi(x)\log x + \mathcal{O}\Big(\frac{x}{\log x}\Big) \ge \frac{1}{4}\,x + o(x) \ge \frac{1}{8}\,x$$

für alle $x \ge x_0$ etwa. Für $2 \le x \le x_0$ gilt

$$\vartheta(x) \ge \log 2 = \tfrac{\log 2}{x}\,x \ge \tfrac{\log 2}{x_0}\,x\,.$$

Mit $c = \min\big\{\frac{1}{8}\,,\ \frac{\log 2}{x_0}\big\} > 0$ folgt nun $\vartheta(x) \ge cx$ für alle $x \ge 2$. □

9.3 Ein Satz von Mertens

Die Reihe

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

divergiert. Wäre sie nämlich konvergent, so käme wegen $1+x+x^2+\cdots = \frac{1}{1-x} \le 1+2x$ für $0 \le x \le \frac{1}{2}$

$$\begin{aligned}\sum_{n\le N} \frac{1}{n} &\le \prod_{p\le N} \left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right) \le \prod_{p\le N} \left(1+\frac{2}{p}\right) \le \prod_{p\le N} e^{2/p} \\ &= \exp\left(2\sum_{p\le N}\frac{1}{p}\right) \le \exp\left(2\sum_{p\in\mathbb{P}}\frac{1}{p}\right) < \infty\end{aligned}$$

bei beliebigem $N \in \mathbb{N}$, was der Divergenz der harmonischen Reihe widerspricht. In der Tat läßt sich mittels partieller Summation aus Satz 2 leicht entnehmen, daß

$$\sum_{p\le x} \frac{1}{p} = \frac{1}{x}\,\pi(x) + \int_2^x \frac{\pi(t)}{t^2}\,dt$$

die Größenordnung $\log\log x$ für $x \ge 4$ besitzt. Wendet man die Chebyshevsche Idee direkt auf $n!$ an, so ergibt sich eine wesentlich schärfere Abschätzung, die von Mertens (1840 - 1927) gefunden wurde.

Satz 3. Für alle $n \in \mathbb{N}$ gilt $\left|\sum_{p\le n} \frac{\log p}{p} - \log n\right| < 3.$

Beweis. Satz 1 liefert

$$\log n! = \sum_{p\le n} \log p \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right] \le n \sum_{p\le n} \log p \sum_{k=1}^{\infty} \frac{1}{p^k} = n \sum_{p\le n} \frac{\log p}{p} + n \sum_{p\le n} \frac{\log p}{p(p-1)}\,.$$

Darin gilt

$$\begin{aligned}\sum_{p\le n} \frac{\log p}{p(p-1)} &\le \sum_{k=2}^{\infty} \frac{\log k}{k(k-1)} = \sum_{\ell=1}^{\infty} \sum_{k=2^{\ell-1}+1}^{2^\ell} \frac{\log k}{k(k-1)} \\ &\le \sum_{\ell=1}^{\infty} \log 2^\ell \sum_{k=2^{\ell-1}+1}^{2^\ell} \left(\frac{1}{k-1}-\frac{1}{k}\right) = \sum_{\ell=1}^{\infty} \frac{\log 2^\ell}{2^\ell} = 2\,\log 2 < 2.\end{aligned}$$

Aus $n! > \left(\frac{n}{e}\right)^n$ für alle $n \in \mathbb{N}$ folgt $\log n! > n\log n - n$, und Zusammenfassung ergibt

$$\log n < 3 + \sum_{p\le n} \frac{\log p}{p}\,. \tag{3}$$

Andererseits hat man

$$\log n! = \sum_{p\le n} \log p \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right] \ge \sum_{p\le n} \log p \left(\frac{n}{p}-1\right) = n \sum_{p\le n} \frac{\log p}{p} - \vartheta(n).$$

Aus $\vartheta(n) < 3n$ gemäß Folgerung 2 und $\log n! \le n \log n$ kommt schließlich

$$\log n \ge -3 + \sum_{p \le n} \frac{\log p}{p}. \tag{4}$$

Die Ungleichungen (3) und (4) ergeben zusammen die Behauptung des Satzes. □

Folgerung 3. Für $x \ge 2$ gilt mit einer gewissen Konstanten c

$$\sum_{p \le x} \frac{\log p}{p} = \log x + \mathcal{O}(1),$$
$$\sum_{p \le x} \frac{1}{p} = \log\log x + c + \mathcal{O}\Big(\frac{1}{\log x}\Big).$$

Nachweis. Satz 3 ergibt für $x \ge 2$

$$\sum_{p \le x} \frac{\log p}{p} = \log[x] + \mathcal{O}(1) = \log x - \log\Big(\frac{[x]}{x}\Big) + \mathcal{O}(1),$$

woraus wegen $\log \frac{x}{[x]} \le \log\big(1 + \frac{1}{[x]}\big) \le \frac{1}{2}$ die erste Behauptung folgt. Partielle Summation liefert damit

$$\begin{aligned}\sum_{p \le x} \frac{1}{p} &= \sum_{p \le x} \frac{\log p}{p} \frac{1}{\log p} = \frac{1}{\log x} \sum_{p \le x} \frac{\log p}{p} + \int_2^x \Big(\sum_{p \le t} \frac{\log p}{p}\Big) \frac{1}{t \log^2 t}\, dt \\ &= \frac{\log x + \mathcal{O}(1)}{\log x} + \int_2^x \frac{\log t + \mathcal{O}(1)}{t \log^2 t}\, dt \\ &= 1 + \mathcal{O}\Big(\frac{1}{\log x}\Big) + \log\log x - \log\log 2 + \int_2^x \frac{\mathcal{O}(1)}{t \log^2 t}\, dt.\end{aligned}$$

Wegen der Konvergenz des Integrals

$$\int_2^\infty \frac{\mathcal{O}(1)}{t \log^2 t}\, dt$$

folgt auch die zweite Behauptung. □

Folgerung 4. Wenn der Grenzwert

$$a = \lim_{x \to \infty} \frac{\vartheta(x)}{x} \Big(= \lim_{x \to \infty} \frac{\psi(x)}{x} = \lim_{x \to \infty} \frac{\pi(x) \log x}{x} \Big)$$

existiert, so gilt $a = 1$.

Nachweis. Mit partieller Summation entsteht

$$\begin{aligned}\sum_{p \le x} \frac{\log p}{p} &= \frac{\vartheta(x)}{x} + \int_2^x \frac{\vartheta(t)}{t^2}\, dt = \mathcal{O}(1) + \int_2^x \Big(\frac{a}{t} + \frac{\mathcal{O}(1)}{t}\Big)\, dt \\ &= a \log x + \mathcal{O}(1) + \int_2^x \frac{\mathcal{O}(1)}{t}\, dt.\end{aligned}$$

Aufspaltung des Integrals bei $\log x$ zeigt für $x \to \infty$

$$\int_2^x \frac{\mathcal{O}(1)}{t}\,dt = \left(\int_2^{\log x} + \int_{\log x}^x\right)\frac{\mathcal{O}(1)}{t}\,dt = \mathcal{O}(\log\log x) + \mathcal{O}(\log x) = \mathcal{O}(\log x).$$

Es folgt

$$\sum_{p\le x}\frac{\log p}{p} = a\log x + \mathcal{O}(\log x),$$

und ein Vergleich mit Folgerung 3 liefert $a = 1$. □

Bemerkung 3. Die Existenz des Grenzwertes aus Folgerung 4 ist Inhalt des 1896 von Hadamard und de la Vallée Poussin mit funktionentheoretischen Methoden bewiesenen Primzahlsatzes

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

Dazu äquivalente Versionen sind $\psi(x) \sim x$ und $\vartheta(x) \sim x$ für $x \to \infty$.

Kapitel 10

Der Dirichletsche Primzahlsatz

Der Beweis des Dirichletschen Primzahlsatzes durch Dirichlet (1805 - 1859) gilt als die Geburtsstunde der analytischen Zahlentheorie. Der Satz besagt, daß in jeder primen Restklasse nach einem festen Modul $q \in \mathbb{N}$ unendlich viele Primzahlen liegen. In diesem Kapitel wird eine quantitative Form bewiesen.

10.1 Restklassencharaktere

Die Dirichletschen Restklassencharaktere ermöglichen die Separierung einer primen Restklasse modulo q aus der primen Restklassengruppe $G(q)$. Sie spielen eine Schlüsselrolle beim Beweis des Dirichletschen Primzahlsatzes.

Definition. Es sei $q \in \mathbb{N}$. Hat $\chi : \mathbb{N} \to \mathbb{C}$ die Eigenschaften

a) χ ist vollständig multiplikativ,

b) $\chi(n) = \chi(m)$ für $n \equiv m \bmod q$,

c) $\chi(n) = 0$ für $(n, q) \neq 1$,

so heißt χ ein Restklassencharakter (Dirichletscher Charakter) mod q. Es bezeichnet $\widehat{G}(q)$ die Menge der Restklassencharaktere mod q.

Bemerkung 1. Es sei $\chi \in \widehat{G}(q)$ und $n \in G(q)$. Dann ist $\chi(n)$ eine $\varphi(q)$-te Einheitswurzel. Dies folgt aus dem kleinen Fermatschen Satz, $n^{\varphi(q)} \equiv 1 \bmod q$, bei Anwendung von χ sowie den Eigenschaften a) und b).

Satz 1. $(\widehat{G}(q), \cdot)$ ist endliche abelsche Gruppe mit $|\widehat{G}(q)| = \varphi(q)$.

Beweis. Die punktweise Multiplikation von Restklassencharakteren mod$q$ ist assoziative und kommutative Verknüpfung auf $\widehat{G}(q)$. Einselement ist der *Hauptcharakter* χ_0 mod q mit

$$\chi_0(n) = \begin{cases} 1 & \text{für } (n,q)=1 \\ 0 & \text{sonst} \end{cases} \qquad (n \in \mathbb{N}).$$

Zu $\chi \in \widehat{G}(q)$ multiplikativ invers ist der *konjugierte Charakter* $\overline{\chi} \in \widehat{G}(q)$ mit

$$\overline{\chi}(n) = \overline{\chi(n)} \qquad (n \in \mathbb{N}),$$

denn offenbar gilt $\chi\overline{\chi} = \chi_0$.

Jeder Restklassencharakter $\chi \in \widehat{G}(q)$ ist wegen b) und c) vollständig durch seine Werte auf der primen Restklassengruppe $G(q)$ bestimmt. Wegen Bemerkung 1 ist also $\widehat{G}(q)$ endlich. Zur Bestimmung der Elementeanzahl verwenden wir das folgende

Lemma 1. Es gilt der Hauptsatz über endliche abelsche Gruppen: Jede endliche abelsche Gruppe ist direktes Produkt zyklischer Untergruppen (die Gruppenverknüpfung sei dabei multiplikativ geschrieben).

Zur Erläuterung sei $(G, \cdot)$ eine endliche abelsche Gruppe mit dem Einselement e. Die zu jedem $g \in G$ eindeutig bestimmte kleinste Zahl $h = h(g) \in \mathbb{N}$ mit $g^h = e$ heißt die Ordnung von g oder der von g erzeugten zyklischen Untergruppe $\{g, g^2, \dots, g^h = e\}$. Gibt es Elemente $g_1, \dots, g_k \in G$ mit den Ordnungen $h_1, \dots, h_k \in \mathbb{N}$ derart, daß jedes $g \in G$ eine eindeutige Darstellung der Gestalt

$$g = g_1^{\lambda_1} \cdots g_k^{\lambda_k} \qquad (0 \le \lambda_\kappa < h_\kappa \text{ für } \kappa = 1, \dots, k)$$

besitzt, so schreibt man

$$G = G_1 \otimes \cdots \otimes G_k$$

mit den von $g_\kappa \in G$ erzeugten zyklischen Untergruppen $G_\kappa = \{g_\kappa, g_\kappa^2, \dots, g_\kappa^{h_\kappa} = e\}$ und nennt G das direkte Produkt von $G_1, \dots, G_k$. Ein induktiver Beweis (einer etwas allgemeineren Version) von Lemma 1 steht bei Hornfeck, Algebra, de Gruyter, Berlin 1971.

Wir setzen den Beweis von Satz 1 fort. Jedes $\chi \in \widehat{G}(q)$ ist durch die Werte $\chi(n)$ mit $n \in G(q)$ eindeutig bestimmt. Infolge Lemma 1 existieren $n_1, \dots, n_k \in G(q)$ mit den Ordnungen $h_1, \dots, h_k \in \mathbb{N}$ derart, daß jedes $n \in G(q)$ eindeutig als Potenzprodukt

$$n = n_1^{\lambda_1} \cdots n_k^{\lambda_k} \qquad (0 \le \lambda_\kappa < h_\kappa \text{ für } \kappa = 1, \dots, k)$$

geschrieben werden kann. Offenbar gilt $\varphi(q) = |G(q)| = h_1 \cdots h_k$. Für jeden Restklassencharakter $\chi \in \widehat{G}(q)$ und jedes $n \in G(q)$ hat man

$$\chi(n) = \big(\chi(n_1)\big)^{\lambda_1} \cdots \big(\chi(n_k)\big)^{\lambda_k},$$

so daß χ durch das k-tupel seiner Werte $\chi(n_\kappa)$ auf den erzeugenden Elementen $n_1, \dots, n_k$ vollständig bestimmt ist. Wegen $n_\kappa^{h_\kappa} = 1$ in $G(q)$ ist $\chi(n_\kappa)$ stets eine h_κ-te Einheitswurzel. Die Anzahl der verschiedenen k-tupel mit dieser Eigenschaft beträgt $h_1 \cdots h_k = \varphi(q)$. Umgekehrt definiert jedes k-tupel, dessen κ-te Komponente eine h_κ-te Einheitswurzel für $\kappa = 1, \dots, k$

ist, auch einen Restklassencharakter $\chi \in \widehat{G}(q)$, und verschiedene derartige k-tupel liefern verschiedene Restklassencharaktere mod q. Daraus kommt die Behauptung. □

Der Beweis von Satz 1 gibt die Anleitung, wie man alle Restklassencharaktere mod q findet. Es ist, entsprechend Lemma 1, ein System von Erzeugenden $n_1, \dots, n_k \in G(q)$ für die direkte Produktzerlegung von $G(q)$ zu bestimmen und mit den entsprechenden Einheitswurzeln zu belegen. Wir geben dazu

Beispiel 1. Die Charaktergruppen $\widehat{G}(q)$ modulo $q = 1, 2, 3, 4, 5$ und $q = 15$ sind gegeben durch

$\widehat{G}(1) = \{\chi_0\}$ mit $\chi_0(1) = 1$, also $\chi_0(n) = 1$ für alle $n \in \mathbb{N}$.

$\widehat{G}(2) = \{\chi_0\}$ mit $\chi_0(1) = 1$, also

$$\chi_0(n) = \begin{cases} 1 & \text{für } 2 \nmid n \\ 0 & \text{für } 2 \mid n\,. \end{cases}$$

$\widehat{G}(3) = \{\chi_0\,,\ \chi_1\}$ mit $\chi_0(2) = 1$ und $\chi_1(2) = -1$, also

$$\chi_0(n) = \begin{cases} 1 & \text{für } n \equiv 1 \bmod 3 \\ 1 & \text{für } n \equiv 2 \bmod 3 \\ 0 & \text{für } n \equiv 0 \bmod 3\,, \end{cases} \qquad \chi_1(n) = \begin{cases} 1 & \text{für } n \equiv 1 \bmod 3 \\ -1 & \text{für } n \equiv 2 \bmod 3 \\ 0 & \text{für } n \equiv 0 \bmod 3\,. \end{cases}$$

$\widehat{G}(4) = \{\chi_0\,,\ \chi_1\}$ mit $\chi_0(3) = 1$ und $\chi_1(3) = -1$, also

$$\chi_0(n) = \begin{cases} 1 & \text{für } 2 \nmid n \\ 0 & \text{für } 2 \mid n\,, \end{cases} \qquad \chi_1(n) = \begin{cases} (-1)^{\frac{n-1}{2}} & \text{für } 2 \nmid n \\ 0 & \text{für } 2 \mid n\,. \end{cases}$$

$\widehat{G}(5) = \{\chi_0\,,\ \chi_1\,,\ \chi_2\,,\ \chi_3\}$ mit $\chi_0(2) = 1\,,\ \chi_1(2) = i\,,\ \chi_2(2) = -1\,,\ \chi_3(2) = -i\,.$

Für $q = 15$ gilt $G(15) = \{1, 2, 4, 7, 8, 11, 13, 14\} = \{1, \underline{2}, 4, 8\} \otimes \{1, \underline{14}\}$, und die acht Charaktere mod 15 sind bestimmt durch die Kombination der Werte $\chi(2) \in \{1, i, -1, -i\}$ mit den Werten $\chi(14) \in \{1, -1\}$.

Bemerkung 2. Die Gruppe $G(q)$ und ihr Dual $\widehat{G}(q)$ sind isomorph. Eine vermittelnde Isomorphieabbildung läßt sich aus der direkten Produktzerlegung $G(q) = G_1 \otimes \cdots \otimes G_k$ mit den Ordnungen $h_\kappa = |G_\kappa|$ und den Erzeugenden n_κ gewinnen. Die Potenzen von χ_κ mit

$$\chi_\kappa(n_\kappa) = \exp\Big(\frac{2\pi i}{h_\kappa}\Big)$$

bilden das Dual $\widehat{G}_\kappa$ von G_κ, und es besteht $\widehat{G}(q) = \widehat{G}_1 \otimes \cdots \otimes \widehat{G}_k$.

Folgerung 1. Es gelten die nachstehenden zueinander dualen Aussagen.

a) Zu jedem $\chi \in \widehat{G}(q)$ mit $\chi \neq \chi_0$ existiert ein $m \in G(q)$ mit $\chi(m) \neq 1$.

b) Zu jedem $n \in G(q)$ mit $n \not\equiv 1 \bmod q$ existiert ein $\psi \in \widehat{G}(q)$ mit $\psi(n) \neq 1$.

Nachweis. a) ist wegen $\chi \neq \chi_0$ klar.

b) folgt aus a) und Bemerkung 2. Ist nämlich $n = n_1^{\lambda_1} \cdots n_k^{\lambda_k} \in G(q)$ mit $0 \leq \lambda_\kappa < h_\kappa$ und (etwa) $\lambda_1 \neq 0$, so wird durch

$$\psi(n_\kappa) = \begin{cases} \exp\left(\frac{2\pi i}{h_1}\right) & \text{für } \kappa = 1 \\ 1 & \text{für } 1 < \kappa \leq k \end{cases}$$

ein $\psi \in \widehat{G}(q)$ mit $\psi(n) = \exp\left(\frac{2\pi\lambda_1 i}{h_1}\right) \neq 1$ bestimmt. □

Satz 2. Es gelten die folgenden Aussagen.

a) Für $\chi \in \widehat{G}(q)$ gilt $\displaystyle\sum_{n \in G(q)} \chi(n) = \begin{cases} \varphi(q) & \text{für } \chi = \chi_0 \\ 0 & \text{sonst.} \end{cases}$

b) Für $n \in G(q)$ gilt $\displaystyle\sum_{\chi \in \widehat{G}(q)} \chi(n) = \begin{cases} \varphi(q) & \text{für } n \equiv 1 \bmod q \\ 0 & \text{sonst.} \end{cases}$

Beweis. Für $\chi = \chi_0$ und $n \equiv 1 \bmod q$ treffen a) und b) offensichtlich zu.

Zu $\chi \neq \chi_0$ existiert nach Folgerung 1 a) ein $m \in G(q)$ mit $\chi(m) \neq 1$. Da mit n auch mn ein primes Restsystem $\bmod q$ durchläuft, folgt

$$\sum_{n \in G(q)} \chi(n) = \sum_{n \in G(q)} \chi(mn) = \chi(m) \sum_{n \in G(q)} \chi(n)$$

und daraus $\displaystyle\sum_{n \in G(q)} \chi(n) = 0$.

Zu $n \not\equiv 1 \bmod q$ existiert nach Folgerung 1 b) ein $\psi \in \widehat{G}(q)$ mit $\psi(n) \neq 1$. Da mit χ auch $\psi\chi$ die Charaktergruppe $\widehat{G}(q)$ durchläuft, folgt

$$\sum_{\chi \in \widehat{G}(q)} \chi(n) = \sum_{\chi \in \widehat{G}(q)} (\psi\chi)(n) = \psi(n) \sum_{\chi \in \widehat{G}(q)} \chi(n)$$

und daraus $\displaystyle\sum_{\chi \in \widehat{G}(q)} \chi(n) = 0$. □

Bemerkung 3. Die Summation in Satz 2 a) darf auch über alle $n \in \mathbb{Z}/q\mathbb{Z}$ oder alle $n \in \mathbb{N}$ eines beliebigen vollständigen Restsystems $\bmod q$ erstreckt werden, und auch die Aussage von Satz 2 b) bleibt richtig, wenn statt $n \in G(q)$ einfach $n \in \mathbb{N}$ vorausgesetzt wird.

Folgerung 2. Es gelten die Orthogonalitätsrelationen für Restklassencharaktere:

a) Für $\psi, \chi \in \widehat{G}(q)$ besteht $\displaystyle\sum_{n \in G(q)} \chi(n)\,\overline{\psi}(n) = \begin{cases} \varphi(q) & \text{für } \chi = \psi \\ 0 & \text{sonst.} \end{cases}$

b) Für $m, n \in G(q)$ besteht $\displaystyle\sum_{\chi \in \widehat{G}(q)} \chi(n)\,\overline{\chi}(m) = \begin{cases} \varphi(q) & \text{für } m \equiv n \bmod q \\ 0 & \text{sonst.} \end{cases}$

Nachweis. Wir haben $\chi(n)\,\overline{\psi}(n) = (\chi\overline{\psi})(n)$ mit $\chi\overline{\psi} = \chi_0$ genau für $\chi = \psi$. Entsprechend gilt $\chi(n)\,\overline{\chi}(m) = \chi(n\,m^{\varphi(q)-1})$ mit $n\,m^{\varphi(q)-1} \equiv 1 \bmod q$ genau für $m \equiv n \bmod q$. Anwendung von Satz 2 liefert die Behauptungen. □

Die Bedeutung der Restklassencharaktere liegt in

Satz 3. Es seien $f \in \mathcal{F}$ und $a, q \in \mathbb{N}$ teilerfremd. Dann gilt für $x > 0$

$$\sum_{\substack{n\le x\\ n\equiv a \bmod q}} f(n) = \frac{1}{\varphi(q)} \sum_{\chi\in\widehat{G}(q)} \overline{\chi}(a) \sum_{n\le x} f(n)\,\chi(n).$$

Beweis. Gemäß Folgerung 2 b) stellt für $a \in \mathbb{N}$ mit $(a, q) = 1$

$$\frac{1}{\varphi(q)} \sum_{\chi\in\widehat{G}(q)} \chi(n)\,\overline{\chi}(a) \qquad (n \in \mathbb{N})$$

die charakteristische Funktion der Menge $\{n \in \mathbb{N} : n \equiv a \bmod q\}$ dar. Einsetzen liefert

$$\sum_{\substack{n\le x\\ n\equiv a \bmod q}} f(n) = \sum_{n\le x} f(n)\,\frac{1}{\varphi(q)} \sum_{\chi\in\widehat{G}(q)} \chi(n)\,\overline{\chi}(a) = \frac{1}{\varphi(q)} \sum_{\chi\in\widehat{G}(q)} \overline{\chi}(a) \sum_{n\le x} f(n)\,\chi(n),$$

wie behauptet. □

10.2 Quantitative Version des Dirichletschen Satzes

Eine quantitative Version des Dirichletschen Primzahlsatzes gibt

Satz 4. Es seien $a, q \in \mathbb{N}$ teilerfremd. Dann gilt für $x \ge 1$

$$\sum_{\substack{p\le x\\ p\equiv a \bmod p}} \frac{\log p}{p} = \frac{1}{\varphi(q)} \log x + \mathcal{O}(1).$$

Bemerkung 4. Sind $a, q \in \mathbb{N}$ nicht teilerfremd, so enthält die arithmetische Progression $a, a+q, a+2q, \ldots$ höchstens eine Primzahl, nämlich a selbst. Satz 4 sagt aus, daß im logarithmischen Mittel in jeder primen Restklasse $\bmod q$ gleichviele Primzahlen liegen. Man kann zeigen

$$\sum_{\substack{p\le x\\ p\equiv a \bmod q}} 1 \sim \frac{1}{\varphi(q)} \frac{x}{\log x} \qquad (x \to \infty);$$

dies liegt allerdings viel tiefer (für $q = 1$ ist es der Primzahlsatz).

Der *Beweis* von Satz 4 verwendet Satz 3,

$$\sum_{\substack{p\le x\\ p\equiv a \bmod q}} \frac{\log p}{p} = \frac{1}{\varphi(q)} \sum_{\chi\in\widehat{G}(q)} \overline{\chi}(a) \sum_{p\le x} \frac{\chi(p)\,\log p}{p}.$$

Dabei gilt für den Hauptcharakter $\chi_0 \in \widehat{G}(q)$ wegen Folgerung 3 aus Kapitel 9

$$\sum_{p\le x} \frac{\chi_0(p)\,\log p}{p} = \sum_{p\le x} \frac{\log p}{p} - \sum_{\substack{p\le x\\ p\mid q}} \frac{\log p}{p} = \log x + \mathcal{O}(1).$$

Da die Anzahl der Restklassencharaktere $\bmod q$ endlich ist, genügt es, zum Beweis von Satz 4 zu zeigen

$$\sum_{p\le x} \frac{\chi(p)\,\log p}{p} = \mathcal{O}(1) \qquad \big(x \ge 1\,,\ \chi_0 \ne \chi \in \widehat{G}(q)\big).$$

Dazu äquivalent ist

$$\sum_{n\le x} \frac{\chi(n)\Lambda(n)}{n} = \mathcal{O}(1) \qquad \big(x \ge 1\,,\ \chi_0 \ne \chi \in \widehat{G}(q)\big), \tag{1}$$

denn es gilt

$$\left|\sum_{n\le x} \frac{\chi(n)\Lambda(n)}{n} - \sum_{p\le x} \frac{\chi(p)\log p}{p}\right| = \left|\sum_{\substack{p^\nu\le x\\ \nu\ge 2}} \frac{\chi(p^\nu)\log p}{p^\nu}\right| \le \sum_p \frac{\log p}{p(p-1)} < 2\,,$$

wobei die letzte Abschätzung etwa dem Beweis von Satz 3 aus Kapitel 9 entnommen werden kann. Dem Nachweis von (1) sind die beiden nächsten Abschnitte gewidmet.

10.3 Dirichletsche L-Reihen

Die analytische Behandlung von multiplikativen Problemen aus der Zahlentheorie basiert zumeist auf den nach Dirichlet benannten Reihen der Form

$$\sum_{n=1}^{\infty} a_n\, n^{-s} \qquad (s \in \mathbb{C}).$$

Wir benötigen hier spezielle Dirichletsche Reihen, deren Koeffizientenfolge ein Restklassencharakter ist und die hier nur für reelles s behandelt werden.

Definition. Es sei $q \in \mathbb{N}$ und $\chi \in \widehat{G}(q)$. Man nennt

$$L(s,\chi) = \sum_{n=1}^{\infty} \chi(n)\, n^{-s} \qquad (s \in \mathbb{R})$$

eine Dirichletsche L-Reihe.

Folgerung 3. Dirichletsche L-Reihen konvergieren absolut für $s > 1$ mit der Eulerschen Produktdarstellung

$$L(s,\chi) = \prod_p \big(1 - \chi(p)\,p^{-s}\big)^{-1}.$$

Für den Hauptcharakter $\chi_0 \in \widehat{G}(q)$ besteht $L(s,\chi_0) = \prod_{p|q} \left(1-p^{-s}\right) \zeta(s)$ sowie

$$\lim_{s\to 1+} (s-1)\, L(s,\chi_0) = \frac{\varphi(q)}{q}\,.$$

Nachweis. Die L-Reihen werden für $s>1$ majorisiert durch $\zeta(s)$. Die Produktdarstellungen kommen deshalb aus Satz 4 und Folgerung 2 aus Kapitel 8. Wegen

$$(n+1)^{-s} < \int_n^{n+1} t^{-s}\,dt < n^{-s} \qquad (n\in\mathbb{N},\ s>1)$$

gilt $\zeta(s) - 1 < \int_1^\infty t^{-s}\,dt = \dfrac{1}{s-1} < \zeta(s)$ oder gleichwertig $1 < (s-1)\,\zeta(s) < s$ für $s>1$. Daraus kommt $(s-1)\,\zeta(s) \sim 1$ für $s\to 1+$ und weiter schließlich die behauptete Limesbeziehung. □

Satz 5. Es sei $\chi_0 \neq \chi \in \widehat{G}(q)$ ein Restklassencharakter $\bmod q$. Dann gelten für $s>0$ die Abschätzungen

a) $$\left|\sum_{x<n\le y} \chi(n)\, n^{-s}\right| \le \varphi(q)\, x^{-s} \qquad (1\le x<y),$$

b) $$\left|\sum_{x<n\le y} \chi(n)\, n^{-s}\,\log n\right| \le \varphi(q)\, x^{-s}\,\log x \qquad (e^{1/s}\le x<y).$$

Beweis. Es handelt sich um Spezialfälle des Dirichletschen Konvergenzkriteriums. Wir setzen

$$A(t) = \sum_{x<\nu\le t} \chi(\nu)$$

und summieren partiell. Wegen $|\chi(\nu)|\le 1$ und Bemerkung 3 ist $A(t)$ beschränkt,

$$|A(t)| \le \varphi(q),$$

und es folgt für $1\le x<y$

$$\begin{aligned}\left|\sum_{x<n\le y} \chi(n)\, n^{-s}\right| &= \left|A(t)\,t^{-s}\Big|_x^y + s\int_x^y A(t)\,t^{-s-1}\,dt\right| \\ &\le \varphi(q)\left(y^{-s} + s\int_x^y t^{-s-1}\,dt\right) = \varphi(q)\,x^{-s}.\end{aligned}$$

Das war in a) behauptet. Analog kommt b) heraus, wobei $t^{-s}\log t$ für $t\ge e^{1/s}$ monoton fällt. □

Folgerung 4. Es sei $\chi_0\neq\chi\in\widehat{G}(q)$ und $\delta>0$. Dann gelten die folgenden Aussagen.

a) Für $s\ge\delta$ konvergiert $L(s,\chi)$ gleichmäßig, und für $s>0$ ist $L(s,\chi)$ stetig.

b) Für $s \geq \delta$ konvergiert $\sum \chi(n)\, n^{-s} \log n$ gleichmäßig, und für $s > 0$ ist $L(s,\chi)$ stetig differenzierbar mit

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

c) Für $s > 1$ konvergieren $L(s,\chi)$ und $L'(s,\chi)$ absolut mit

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

d) Für $s > 1$ ist $L(s,\chi) \neq 0$.

Nachweis. Es sind a), b) direkte Konsequenzen aus Satz 5. In c) ist die absolute Konvergenz der Reihen $L(s,\chi)$ und $L'(s,\chi)$ für $s > 1$ klar, ebenso die der Reihen $\sum \mu(n)\,\chi(n)\, n^{-s}$ und $\sum \chi(n)\,\Lambda(n)\, n^{-s}$ wegen $|\mu(n)\,\chi(n)| \leq 1$ und $|\chi(n)\,\Lambda(n)| \leq \log n$. Die behaupteten Identitäten kommen aus den Faltungsdarstellungen

$$\chi * (\mu\,\chi) = \chi\,(1 * \mu) = \varepsilon \quad \text{ und } \quad \chi * (\chi\,\Lambda) = \chi\,(1 * \Lambda) = \chi \log$$

sowie Satz 4 a) aus Kapitel 8. Schließlich folgt d) aus der ersten Identität in c). □

Über Folgerung 4 d) hinaus geht der

Satz 6. Für $\chi_0 \neq \chi \in \widehat{G}(q)$ besteht $L(1,\chi) \neq 0$.

Den Beweis von Satz 6 führen wir im nächsten Abschnitt. Hier zeigen wir, daß (1) aus Satz 6 folgt: Wegen $\log = 1 * \Lambda$ gilt nämlich

$$\sum_{n\leq x} \frac{\chi(n)\,\log n}{n} = \sum_{n\leq x} \frac{\chi(n)}{n} \sum_{d\mid n} \Lambda(d) = \sum_{d\leq x} \frac{\chi(d)\,\Lambda(d)}{d} \sum_{m\leq \frac{x}{d}} \frac{\chi(m)}{m}\,. \tag{2}$$

Wegen Satz 5 a) wissen wir

$$\sum_{m\leq x/d} \frac{\chi(m)}{m} = L(1,\chi) + \mathcal{O}\Big(\frac{d}{x}\Big),$$

und Folgerung 2 aus Kapitel 9 liefert weiter

$$\sum_{d\leq x} \frac{\chi(d)\,\Lambda(d)}{d}\, \mathcal{O}\Big(\frac{d}{x}\Big) = \mathcal{O}\Big(\frac{1}{x} \sum_{d\leq x} \Lambda(d)\Big) = \mathcal{O}(1).$$

Da $L'(1,\chi)$ konvergiert, besteht andererseits

$$\sum_{n\leq x} \frac{\chi(n)\,\log n}{n} = \mathcal{O}(1),$$

und Einsetzen in (2) ergibt insgesamt

$$L(1,\chi) \sum_{d\leq x} \frac{\chi(d)\,\Lambda(d)}{d} = \mathcal{O}(1).$$

Aus Satz 6 folgt daher (1), wie behauptet. □

10.4 Beweis von Satz 6

Lemma 2. Es seien $a, q \in \mathbb{N}$ teilerfremd und h die Ordnung von a in $G(q)$. Dann ist $\chi(a)$ für jeden Restklassencharakter $\chi \in \widehat{G}(q)$ eine h-te Einheitswurzel, und jede h-te Einheitswurzel wird gleich oft angenommen, wenn χ die Restklassencharaktere mod$q$ durchläuft.

Beweis. Wegen $(\chi(a))^h = \chi(a^h) = \chi(1) = 1$ ist der erste Teil der Behauptung trivial. Aus $a \equiv 1 \bmod q$ folgt $h = 1$ und $\chi(a) = 1$ für jedes $\chi \bmod q$, so daß nichts zu zeigen ist. Es sei also $a \not\equiv 1 \bmod q$, also auch $h > 1$. Weiter sei $\xi \in \mathbb{C}$ eine h-te Einheitswurzel. Wir betrachten die Summe

$$S = \sum_{\lambda=0}^{h-1} \sum_{\chi \in \widehat{G}(q)} \Big(\frac{\chi(a)}{\xi}\Big)^{\lambda}.$$

Wegen Satz 2 b) gilt

$$\sum_{\chi \in \widehat{G}(q)} \chi\big(a^{\lambda}\big) = \begin{cases} \varphi(q) & \text{für } a^{\lambda} \equiv 1 \bmod q \\ 0 & \text{sonst,} \end{cases}$$

wobei nach Voraussetzung $a^{\lambda} \equiv 1 \bmod q$ mit $0 \le \lambda < h$ genau für $\lambda = 0$ zutrifft. Es folgt daher

$$S = \sum_{\lambda=0}^{h-1} \frac{1}{\xi^{\lambda}} \sum_{\chi \in \widehat{G}(q)} \chi(a^{\lambda}) = \varphi(q) \sum_{\substack{\lambda=0 \\ a^{\lambda} \equiv 1 \bmod q}}^{h-1} \frac{1}{\xi^{\lambda}} = \varphi(q).$$

Andererseits ist mit ξ auch $\eta = \frac{\chi(a)}{\xi}$ eine h-te Einheitswurzel, und es gilt

$$\sum_{\lambda=0}^{h-1} \eta^{\lambda} = \begin{cases} \frac{1-\eta^h}{1-\eta} = 0 & \text{für } \eta \neq 1 \\ h & \text{für } \eta = 1, \end{cases}$$

wobei $\eta = 1$ genau für $\chi(a) = \xi$ eintritt. Es folgt

$$S = \sum_{\chi \in \widehat{G}(q)} \sum_{\lambda=0}^{h-1} \Big(\frac{\chi(a)}{\xi}\Big)^{\lambda} = h \sum_{\substack{\chi \in \widehat{G}(q) \\ \chi(a) = \xi}} 1.$$

Zusammenfassung ergibt für die gesuchte Anzahl

$$\sum_{\substack{\chi \in \widehat{G}(q) \\ \chi(a) = \xi}} 1 = \frac{\varphi(q)}{h},$$

wie behauptet. □

Wir benötigen die folgende Konsequenz aus Lemma 2.

Folgerung 5. Es gelten die Aussagen:

a) Für $s > 1$ ist $\prod_{\chi \in \widehat{G}(q)} L(s,\chi) \geq 1$.

b) Es gibt höchstens einen Restklassencharakter $\chi \in \widehat{G}(q)$ mit $L(1,\chi) = 0$; dieser ist reell.

Nachweis. a) Wegen Folgerung 3 besteht für $s > 1$

$$\prod_{\chi \in \widehat{G}(q)} L(s,\chi) = \prod_{\chi \in \widehat{G}(q)} \prod_p \left(1 - \chi(p)\, p^{-s}\right)^{-1} = \prod_p \left(\prod_{\chi \in \widehat{G}(q)} \left(1 - \chi(p)\, p^{-s}\right) \right)^{-1}.$$

Für $p \mid q$ gilt $\chi(p) = 0$, also $\prod_{\chi \in \widehat{G}(q)} \left(1 - \chi(p)\, p^{-s}\right) = 1$. Für $p \nmid q$ gilt mit der Ordnung $h \in \mathbb{N}$ von p in $G(q)$, $\xi = \exp\left(\frac{2\pi i}{h}\right)$ und $z = p^{-s}$ gemäß Lemma 2

$$\prod_{\chi \in \widehat{G}(q)} \left(1 - \chi(p)\, p^{-s}\right) = \left(\prod_{\lambda=0}^{h-1} \left(1 - \xi^\lambda z\right) \right)^{\frac{\varphi(q)}{h}} = \left(1 - z^h\right)^{\frac{\varphi(q)}{h}} = \left(1 - p^{-hs}\right)^{\frac{\varphi(q)}{h}} \leq 1.$$

Daraus folgt a).

b) Angenommen, für die verschiedenen Charaktere $\chi_1\,,\ \chi_2 \in \widehat{G}(q)$ mit $\chi_0 \neq \chi_1\,,\ \chi_2$ gilt $L(1,\chi_1) = L(1,\chi_2) = 0$. Dann liefert a) für $s > 1$

$$(3) \qquad \frac{1}{s-1} \leq \frac{1}{s-1} \prod_{\chi \in \widehat{G}(q)} L(s,\chi) = (s-1)\, L(s,\chi_0)\, \frac{L(s,\chi_1)}{s-1}\, \frac{L(s,\chi_2)}{s-1} \prod_{\substack{\chi \in \widehat{G}(q) \\ \chi \neq \chi_0,\chi_1,\chi_2}} L(s,\chi).$$

Wegen Folgerung 3 existiert

$$\lim_{s \to 1+} (s-1)\, L(s,\chi_0) = \frac{\varphi(q)}{q}.$$

Aus Folgerung 4 b) kommt für $j = 1, 2$ die Existenz von

$$\lim_{s \to 1+} \frac{L(s,\chi_j)}{s-1} = \lim_{s \to 1+} \frac{L(s,\chi_j) - L(1,\chi_j)}{s-1} = L'(1,\chi_j)$$

sowie wegen Folgerung 4 a)

$$\lim_{s \to 1+} \prod_{\substack{\chi \in \widehat{G}(q) \\ \chi \neq \chi_0,\chi_1,\chi_2}} L(s,\chi) = \prod_{\substack{\chi \in \widehat{G}(q) \\ \chi \neq \chi_0,\chi_1,\chi_2}} L(1,\chi).$$

Daher ist die rechte Seite von (3) für $s \to 1+$ beschränkt, die linke Seite ist dagegen unbeschränkt. Für höchstens ein $\chi \in \widehat{G}(q)$ gilt folglich $L(1,\chi) = 0$. Da $L(1,\chi) = 0$ stets $L(1,\overline{\chi}) = 0$ nach sich zieht, muß nach dem schon bewiesenen Teil $\chi = \overline{\chi}$ gelten, der Charakter $\chi \in \widehat{G}(q)$ also reell sein. □

Lemma 3. Es sei $\chi \neq \chi_0$ ein reeller Restklassencharakter mod q. Dann gilt $L(1,\chi) \neq 0$.

Beweis. Hier verlassen wir den von Dirichlet eingeschlagenen Weg und folgen Mertens (1897). Wegen Satz 2 aus Kapitel 7 ist

$$f = 1 * \chi$$

multiplikativ, und es gilt

$$f(p^\nu) = 1 + \chi(p) + \cdots + (\chi(p))^\nu = \begin{cases} \frac{1-(\chi(p))^{\nu+1}}{1-\chi(p)} & \text{für } \chi(p) \in \{0,-1\} \\ \nu+1 & \text{für } \chi(p) = 1\,, \end{cases}$$

also jedenfalls $f(p^\nu) \geq 0$ und damit $f(n) \geq 0$ für alle $n \in \mathbb{N}$. Weiter gilt $f(p^{2\nu}) \geq 1$ für alle $\nu \in \mathbb{N}$ und damit sogar $f(m^2) \geq 1$ für alle $m \in \mathbb{N}$. Insbesondere ist wegen

$$\sum_{n\leq x} \frac{f(n)}{\sqrt{n}} \geq \sum_{m\leq\sqrt{x}} \frac{f(m^2)}{m} \geq \sum_{m\leq\sqrt{x}} \frac{1}{m}$$

die Reihe $\displaystyle\sum_{n=1}^{\infty} \frac{f(n)}{\sqrt{n}}$ unbeschränkt.

Andererseits haben wir aber

$$\begin{aligned} \sum_{n\leq x} \frac{f(n)}{\sqrt{n}} &= \sum_{n\leq x} \frac{1}{\sqrt{n}} \sum_{d|n} \chi(d) = \sum_{md\leq x} \frac{\chi(d)}{\sqrt{d}\sqrt{m}} \\ &= \sum_{d\leq\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \sum_{m\leq x/d} \frac{1}{\sqrt{m}} + \sum_{\sqrt{x}<d\leq x} \frac{\chi(d)}{\sqrt{d}} \sum_{m\leq x/d} \frac{1}{\sqrt{m}} \\ &= \sum_{d\leq\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \sum_{m\leq x/d} \frac{1}{\sqrt{m}} + \sum_{m\leq\sqrt{x}} \frac{1}{\sqrt{m}} \sum_{\sqrt{x}<d\leq x/m} \frac{\chi(d)}{\sqrt{d}} \\ &=: \sum\nolimits_1 + \sum\nolimits_2. \end{aligned}$$

Nach Satz 2 aus Kapitel 8 und Satz 5 a) ist darin

$$\begin{aligned} \sum\nolimits_1 &= \sum_{d\leq\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \Big(2\sqrt{\frac{x}{d}} + \gamma_{\frac{1}{2}} + \mathcal{O}\Big(\sqrt{\frac{d}{x}}\Big)\Big) \\ &= 2\sqrt{x} \sum_{d\leq\sqrt{x}} \frac{\chi(d)}{d} + \gamma_{\frac{1}{2}} \sum_{d\leq\sqrt{x}} \frac{\chi(d)}{\sqrt{d}} + \mathcal{O}\Big(\frac{1}{\sqrt{x}} \sum_{d\leq\sqrt{x}} 1\Big) \\ &= 2\sqrt{x}\, L(1,\chi) + \mathcal{O}(1). \end{aligned}$$

Ebenso bekommen wir

$$\sum\nolimits_2 = \sum_{m\leq\sqrt{x}} \frac{1}{\sqrt{m}}\, \mathcal{O}\Big(\frac{1}{\sqrt[4]{x}}\Big) = \mathcal{O}(1).$$

Beides zusammen ergibt

$$\sum_{n\leq x} \frac{f(n)}{\sqrt{n}} = 2\sqrt{x}\, L(1,\chi) + \mathcal{O}(1).$$

Wäre nun $L(1,\chi) = 0$, so wäre $\displaystyle\sum_{n=1}^{\infty} \frac{f(n)}{\sqrt{n}}$ beschränkt. Dieser Widerspruch zeigt die Behauptung von Lemma 3 und vervollständigt den Beweis des Dirichletschen Primzahlsatzes. □

Kapitel 11

Partitionen

In diesem Kapitel werden additive Zerlegungen natürlicher Zahlen betrachtet und der Pentagonalzahlensatz von Euler und Legendre sowie die logarithmische Version der asymptotischen Partitionenformel von Hardy und Ramanujan bewiesen.

11.1 Partitionsfunktionen

Das Grundproblem der additiven Zahlentheorie besteht bei gegebenen Mengen $A, B \subseteq \mathbb{Z}$ in der Charakterisierung der Summenmenge $A + B = \{a + b : a \in A\,,\ b \in B\}$.

Beispiel 1. Additive Aussagen sind etwa:

a) Der Vier-Quadrate-Satz von Lagrange beinhaltet die Gleichung $\mathbb{N}_0 = A + A + A + A$ wobei $A = \{n^2 : n \in \mathbb{N}_0\}$ die Menge der Quadratzahlen ist.

b) Die Lösung des Waringschen Problems durch Hilbert (1909) lautet, daß zu jeder Zahl $k \in \mathbb{N} \setminus \{1\}$ ein $g(k) \in \mathbb{N}$ existiert mit $\mathbb{N}_0 = A + \cdots + A$ mit $g(k)$ Summanden, wobei $A = \{n^k : n \in \mathbb{N}_0\}$ die Menge der k-ten Potenzen ist.

c) Die bislang unbewiesene Goldbach-Vermutung aus dem Jahre 1742 besagt $A + A = \{2n : n \in \mathbb{N},\ n > 2\}$, wobei $A = \mathbb{P} \setminus \{2\}$ die Menge der ungeraden Primzahlen bezeichnet. Vinogradov zeigte 1937 die Existenz eines $n_0 \in \mathbb{N}$ mit der Eigenschaft $\{n \in \mathbb{N} : n \geq n_0\,,\ 2 \nmid n\} \subseteq A + A + A$, und Chen bewies 1966 die Existenz eines $n_0 \in \mathbb{N}$ mit $\{n \in \mathbb{N} : n \geq n_0\,,\ 2|n\} \subseteq A + B$, wobei $B = A \cup \{pp' : p, p' \in A\}$ nur ungerade Primzahlen und Produkte zweier ungerader Primzahlen enthält.

Von Interesse ist oft die Anzahl der Darstellungen von $n \in \mathbb{N}_0$ als Summe $n = a+b$ mit $a \in A$, $b \in B$. Offenbar gilt $n \in A + B$ genau dann, wenn die Darstellungsanzahl nicht verschwindet. Bei den Partitionsfunktionen $p(n)$ und $p_k(n)$ treffen wir diese Situation an.

Definition. Für $n \in \mathbb{N}$ und $k \in \mathbb{N}$ bezeichnen $p(n)$ und $p_k(n)$ die Anzahl der Darstellungen von n als Summe von beliebig vielen bzw. von höchstens k natürlichen Zahlen. Dabei

werden zwei Darstellungen als gleich angesehen, wenn sie sich nur durch die Reihenfolge der Summanden unterscheiden. Ferner setzt man $p(0) = p_k(0) = 1$.

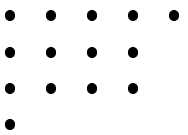
Beispiel 2. Offenbar gelten $p(1) = p_k(1) = 1$ und $1 = p_1(n) < p_2(n) < \cdots < p_n(n) = p(n)$ für alle $k, n \in \mathbb{N}$. Man erhält etwa $p(2) = 2$, $p(3) = 3$, $p(4) = 5$, $p(5) = 7$ sowie $p_3(5) = 5$.

Es sei nun

$$n = n_1 + \cdots + n_k \quad \text{mit} \quad n_1 \geq n_2 \geq \ldots \geq n_k > 0$$

eine Partition von n. Sie läßt sich durch ein Diagramm aus zeilen- und spaltenweise angeordneten Punkten veranschaulichen, welches in der j-ten Zeile genau n_j Punkte enthält.

$14 = 5 + 4 + 4 + 1$



$14 = 4 + 3 + 3 + 3 + 1$

Liest man das Diagramm vertikal, so erhält man wieder eine Partition von n, die zur Ausgangspartition konjugierte Partition

$$\begin{aligned} n = & \underbrace{k + \cdots + k}_{n_k \text{ Summanden}} + \underbrace{\big((k-1) + \cdots + (k-1)\big)}_{n_{k-1} - n_k \text{ Summanden}} + \cdots + \underbrace{(1 + \cdots + 1)}_{n_1 - n_2 \text{ Summanden}}, \\ & = n_k \cdot k + (n_{k-1} - n_k) \cdot (k-1) + \cdots + (n_1 - n_2) \cdot 1\,, \end{aligned}$$

wobei der größte Summand gleich k ist. Die durch Konjugation erklärte Abbildung ist offenbar bijektiv. Damit erhält man

Satz 1. Die Anzahl der Partitionen von n in genau k natürliche Summanden ist gleich der Anzahl der Partitionen von n, deren größter Summand k ist. Die Anzahl $p_k(n)$ der Partitionen von n in höchstens k natürliche Summanden ist gleich der Anzahl der Partitionen mit Summanden $\leq k$.

Folgerung 1. Es gilt

$$p_k(n) = \sum_{\substack{(\lambda_1, \ldots, \lambda_k) \in \mathbb{N}_0^k \\ 1 \cdot \lambda_1 + 2 \cdot \lambda_2 + \cdots + k \cdot \lambda_k = n}} 1\,.$$

Demnach kann die Bestimmung von $p_k(n)$ als eine Abzählaufgabe von Lösungen einer diophantischen Gleichung aufgefaßt werden.

Folgerung 2. Es gilt die Rekursionsformel

$$p_k(n) = \sum_{\lambda=0}^{\left[\frac{n}{k}\right]} p_{k-1}(n - \lambda k),$$

speziell $p_1(n) = 1$, $p_2(n) = \left[\frac{n}{2}\right] + 1$, $p_3(n) = p_2(n) + p_2(n-3) + \cdots + p_2\big(n - 3\left[\frac{n}{3}\right]\big)$.

11.2 Erzeugende Potenzreihen

Das Aufsummieren von [ ]-Symbolen gemäß Folgerung 2 wird schnell ziemlich unhandlich. Eine ganz andersartige Methode zur Bestimmung von $p_k(n)$ beruht auf der Verwendung von Potenzreihen.

Satz 2. Für $k \in \mathbb{N}_0$ und $|x| < 1$ besteht

$$\prod_{j=1}^{k} \frac{1}{1-x^j} = \sum_{n=0}^{\infty} p_k(n)\, x^n.$$

Beweis. Für $|x| < 1$ konvergieren die geometrischen Reihen in x^j absolut und dürfen ausmultipliziert und umgeordnet werden. Es gilt

$$\prod_{j=1}^{k} \frac{1}{1-x^j} = \prod_{j=1}^{k} \left(1 + x^j + x^{2j} + \cdots\right) = \sum_{\lambda_1,\lambda_2,\ldots,\lambda_k=0}^{\infty} x^{\lambda_1+2\lambda_2+\cdots+k\lambda_k} = \sum_{n=0}^{\infty} p_k(n)\, x^n,$$

letzteres wegen Folgerung 1. □

Beispiel 3. Bezeichnet $\langle x \rangle$ die zu $x \in \mathbb{R}$ mit $2x \notin \mathbb{Z}$ nächstgelegene ganze Zahl, so gilt

$$p_3(n) = \Big[\frac{(n+1)(n+5)}{12}\Big] = \Big\langle \frac{(n+3)^2}{12} \Big\rangle.$$

Denn Satz 2 liefert für $|x| < 1$

$$f_3(x) = \frac{1}{(1-x)(1-x^2)(1-x^3)} = \sum_{n=0}^{\infty} p_3(n)\, x^n.$$

Mit $\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ lautet die Partialbruchzerlegung von $f_3(x)$:

$$\begin{aligned} f_3(x) &= \frac{1}{(1-x)^3(1+x)(1-\omega x)(1-\omega^2 x)} \\ &= \frac{\frac{1}{6}}{(1-x)^3} + \frac{\frac{1}{4}}{(1-x)^2} + \frac{\frac{17}{72}}{1-x} + \frac{\frac{1}{8}}{1+x} + \frac{1}{9}\Big(\frac{1}{1-\omega x} + \frac{1}{1-\omega^2 x}\Big). \end{aligned}$$

Reihenentwicklung der Partialbrüche und Zusammenfassung ergibt

$$f_3(x) = \sum_{n=0}^{\infty} \Big(\frac{(n+2)(n+1)}{12} + \frac{n+1}{4} + \frac{17}{72} + \frac{(-1)^n}{8} + \frac{\omega^n + \omega^{-n}}{9}\Big)\, x^n.$$

Durch Koeffizientenvergleich folgt

$$\begin{aligned} p_3(n) &= \frac{n^2+6n+5}{12} + \frac{17}{72} + \frac{(-1)^n}{8} + \frac{\omega^n + \omega^{-n}}{9} \\ &= \frac{(n+1)(n+5)}{12} + \varrho_1(n) = \frac{(n+3)^2}{12} + \varrho_2(n) \end{aligned}$$

mit $0 \le \varrho_1(n) < 1$ und $|\varrho_2(n)| \le \frac{1}{2}$, woraus die obigen Formeln kommen.

Durch Satz 2 wird der folgende Sachverhalt nahegelegt.

Satz 3. (Euler) Für $|x| < 1$ gilt

$$\prod_{k=1}^{\infty} \frac{1}{1-x^k} = \sum_{n=0}^{\infty} p(n)x^n.$$

Beweis. a) Für $|x| < 1$ konvergiert das Produkt absolut. Denn bei festem x mit $0 \le x < 1$ sind die Partialprodukte $f_k(x)$ monoton wachsend und beschränkt wegen

$$1 \le \prod_{j=1}^{k} \frac{1}{1-x^j} = \exp\left(\sum_{j=1}^{k} \log \frac{1}{1-x^j}\right) = \exp\left(\sum_{j=1}^{k}\sum_{\nu=1}^{\infty} \frac{x^{j\nu}}{\nu}\right) \le \exp\left(\sum_{\nu=1}^{\infty}\sum_{j=1}^{\infty} x^{j\nu}\right)$$
$$= \exp\left(\sum_{\nu=1}^{\infty} \frac{x^\nu}{1-x^\nu}\right) \le \exp\left(\frac{1}{1-x}\sum_{\nu=1}^{\infty} x^\nu\right) = \exp\left(\frac{x}{(1-x)^2}\right).$$

b) Wir zeigen die Existenz von

$$f(x) = \sum_{n=0}^{\infty} p(n)\, x^n$$

für $|x| < 1$. Es genügt, dies für $0 \le x < 1$ zu erledigen. Bei festem x wächst die Folge der Partialsummen $\sum_{n=0}^{k} p(n)\, x^n$ monoton. Aus Satz 2 und Teil a) folgt deren Beschränktheit, denn

$$1 \le \sum_{n=0}^{k} p(n)\, x^n < \sum_{n=0}^{k} p(n)\, x^n + \sum_{n=k+1}^{\infty} p_k(n)\, x^n = \sum_{n=0}^{\infty} p_k(n)\, x^n$$
$$= f_k(x) = \prod_{j=1}^{k} \frac{1}{1-x^j} < \prod_{j=1}^{\infty} \frac{1}{1-x^j}\,.$$

Also konvergiert $\sum_{n=0}^{\infty} p(n)x^n = f(x)$ für $|x| < 1$.

c) Aus b) sieht man für $0 \le x < 1$

$$\sum_{n=0}^{k} p(n)\, x^n < f_k(x) < f(x) = \sum_{n=0}^{\infty} p(n)x^n,$$

also $\lim_{k\to\infty} f_k(x) = f(x)$. Damit kommt

$$\sum_{n=0}^{\infty} p(n)x^n = f(x) = \lim_{k\to\infty} f_k(x) = \lim_{k\to\infty} \prod_{j=1}^{k} \frac{1}{1-x^j} = \prod_{j=1}^{\infty} \frac{1}{1-x^j}\,,$$

wie behauptet. □

Bemerkung 1. Zieht man funktionentheoretische Hilfsmittel hinzu, so sieht man

$$f(z) = \sum_{n=0}^{\infty} p(n)\, z^n = \prod_{k=1}^{\infty} \frac{1}{1-z^k} \qquad (z \in \mathbb{C},\ |z| < 1).$$

Die Cauchyschen Integralformeln liefern die Darstellung

$$p(n) = \frac{f^{(n)}(0)}{n!} = \frac{1}{2\pi i} \int_{\mathsf{k}} \frac{f(z)}{z^{n+1}}\, dz\,,$$

wobei k ein einfach geschlossener, positiv orientierter Kreis um 0 vom Radius $r < 1$ ist. Bei geeigneter Wahl von r und sogenannter Farey-Zerschneidung (Farey, 1766 - 1826) der Spur von k läßt sich mit der Hardy-Littlewoodschen Kreismethode die berühmte Partitionenformel

$$p(n) \sim \frac{1}{4n\sqrt{3}} \exp\left(\pi \sqrt{\frac{2n}{3}}\right) \qquad (n \to \infty)$$

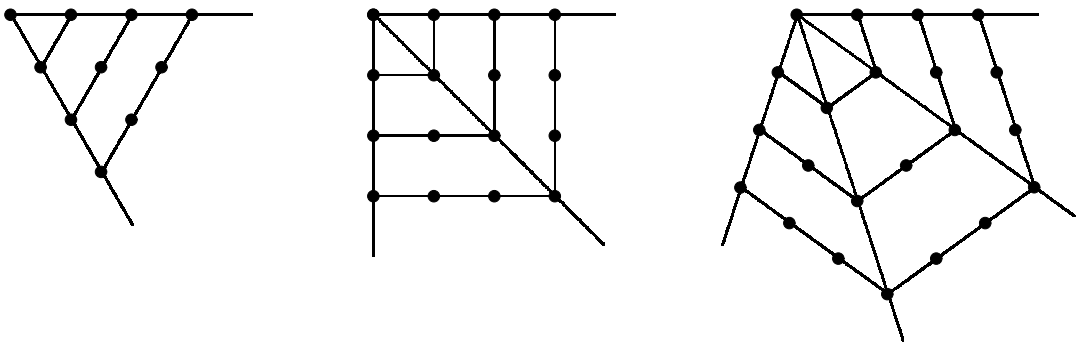
von Hardy und Ramanujan gewinnen. Eine (schwächere) asymptotische Formel für $\log p(n)$ wird am Schluß dieses Kapitels bewiesen.

11.3 Der Euler-Legendresche Pentagonalzahlensatz

Wegen Satz 3 konvergiert für $|x| < 1$ das unendliche Produkt $\prod_{k=1}^{\infty} \left(1 - x^k\right)$. Der Pentagonalzahlensatz von Euler und Legendre liefert die Potenzreihenentwicklung dieses Produkts.

Definition. Es sei $3 \leq k \in \mathbb{N}$. Die Zahlen $n + (k-2)\binom{n}{2}$ mit $n \in \mathbb{N}$ heißen k-Eck-Zahlen.

Bemerkung 2. Die folgenden Punktediagramme für $k = 3, 4, 5$ erläutern die Bezeichnung.



Die k-Eck-Zahlen sind die Partialsummen der arithmetischen Folge

$$1\,,\ 1 + (k-2)\,,\ 1 + 2(k-2)\,,\ 1 + 3(k-2)\,, \ldots\,,$$

also die Zahlen

$$\sum_{\nu=1}^{n} \big(1 + (\nu - 1)(k-2)\big) = n + (k-2)\binom{n}{2}.$$

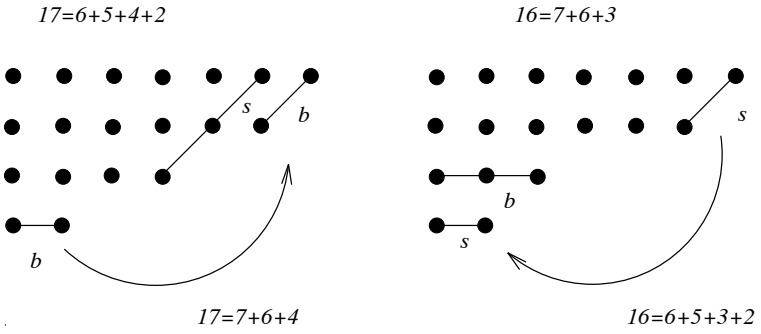
Für $k = 3$ enthält man die Dreieckzahlen $\frac{n(n+1)}{2}$, für $k = 4$ die Quadratzahlen, für $k = 5$ die Fünfeckzahlen $\beta(n) = \frac{3n^2-n}{2}$. Man sieht $\beta(-n) = \frac{3n^2+n}{2}$ sowie $\beta(n) < \beta(-n) < \beta(n+1)$ für $n \in \mathbb{N}$. Die paarweise verschiedenen Zahlen $\beta(\pm n)$ mit $n \in \mathbb{N}$ nennt man *Pentagonalzahlen*.

Satz 4. (Euler-Legendrescher Pentagonalzahlensatz) Es seien $G(n)$ und $U(n)$ die Anzahl der Partitionen von n in eine gerade bzw. eine ungerade Anzahl paarweise verschiedener natürlicher Summanden. Dann gilt

$$G(n) - U(n) = \begin{cases} 0 & \text{für } n \neq \beta(\pm\lambda) \\ (-1)^\lambda & \text{für } n = \beta(\pm\lambda) \end{cases} \qquad (\lambda \in \mathbb{N}).$$

Beweis. Neben Beweisen von Euler (1750), Legendre (1830), Jacobi (1846) gibt es einen hübschen kombinatorischen Beweis von Franklin (1881), den wir im folgenden behandeln.

Wir betrachten im Punktediagramm Partitionen von $n \in \mathbb{N}$ in paarweise verschiedene Summanden. Etwa ist eine solche Partition von 17 gegeben durch



Dabei wird s als Seite, b als Basis bezeichnet. Wir definieren eine Operation T durch Anlegen von b an s oder von s an b, so daß die neue Partition von n wieder paarweise verschiedene Summanden enthält, die zeilenweise der Größe nach geordnet sind. Wenn T durchführbar ist, so gibt es die beiden Möglichkeiten

$$\begin{aligned} T = T_1: &\quad \text{Lege } b \text{ an } s \text{ an,} \\ T = T_2: &\quad \text{Lege } s \text{ an } b \text{ an.} \end{aligned}$$

Wenn T_1 möglich ist, so gilt $b \leq s$. Falls $T = T_2$ möglich ist, so gilt $s < b$. Wenn also T überhaupt durchführbar ist, dann eindeutig. In diesem Fall ordnet T einer geraden Partition von n bijektiv eine ungerade zu und umgekehrt. Wir untersuchen, wann T durchführbar ist.

a) $s > b$: $T = T_1$ ist stets durchführbar.

b) $s = b$: $T = T_1$ ist durchführbar, es sei denn, s und b haben einen Punkt gemeinsam. Dies tritt genau dann ein, wenn
$$n = b + (b+1) + \cdots + (b + (b-1)) = \tfrac{b}{2}(3b-1) = \beta(b).$$

c) $s < b$: $T = T_2$ ist durchführbar, es sei denn, $s = b - 1$ und s, b haben einen Punkt gemeinsam. Dies ist genau dann der Fall, wenn
$$n = (s+1) + (s+2) + \cdots + (s+s) = \tfrac{s}{2}\,(3s+1) = \beta(-s).$$

Die Ausnahmezahlen vom Typ b) und c) sind paarweise verschieden. Mit $\lambda \in \mathbb{N}$ folgt:

a) Für $n \notin \beta(\mathbb{Z})$ gilt $G(n) = U(n)$.

b) Für $n = \beta(\lambda)$ gilt $G(n) - U(n) = (-1)^\lambda$.

c) Für $n = \beta(-\lambda)$ gilt $G(n) - U(n) = (-1)^\lambda$.

Das war behauptet. □

Als Konsequenz aus Satz 4 kommt

Satz 5. (Euler) Für $|x| < 1$ gilt
$$\prod_{k=1}^{\infty} (1 - x^k) = 1 + \sum_{\lambda \geq 1} (-1)^\lambda \left(x^{\beta(\lambda)} + x^{\beta(-\lambda)} \right) =: \sum_{\lambda=-\infty}^{\infty} (-1)^\lambda \, x^{\frac{\lambda}{2}(3\lambda-1)}\,.$$

Beweis. Der Koeffizient von x^n entsteht durch Ausmultiplikation von
$$(1-x)(1-x^2)\cdots(1-x^n).$$
Er ist offenbar $G(n) - U(n)$, und die Behauptung kommt aus Satz 4. □

Zusammen mit Satz 3 ermöglicht der Satz 5 nun eine rasche rekursive Berechnung von $p(n)$.

Folgerung 3. Für $n \in \mathbb{N}$ gilt
$$p(0) = 1\,, \quad p(n) = \sum_{\lambda \geq 1}^{*} (-1)^{\lambda+1} \Big(p(n - \beta(\lambda)) + p(n - \beta(-\lambda)) \Big),$$
wobei $*$ anzeigt, daß $p(-m) = 0$ für $m \in \mathbb{N}$ einzusetzen ist.

Nachweis. Die Sätze 3 und 5 liefern für $|x| < 1$:
$$\sum_{n=0}^{\infty} p(n)\, x^n \left(1 + \sum_{\lambda=1}^{\infty} (-1)^\lambda \left(x^{\beta(\lambda)} + x^{\beta(-\lambda)} \right) \right) = 1.$$
Ausmultiplizieren der Reihen und Koeffizientenvergleich ergibt $p(0) = 1$ sowie für $n \in \mathbb{N}$ die behauptete Rekursionsgleichung. □

Beispiel 4. Die ersten Pentagonalzahlen sind

λ	1	2	3	4	5	6	...
$\beta(\lambda)$	1	5	12	22	35	51	...
$\beta(-\lambda)$	2	7	15	26	40	57	...

Damit wird

$$\begin{aligned} p(n) = &+ p(n-1) + p(n-2) - p(n-5) - p(n-7) \\ &+ p(n-12) + p(n-15) - p(n-22) - p(n-26) \\ &+ p(n-35) + p(n-40) - p(n-51) - p(n-57) + + - - \cdots , \end{aligned}$$

und man berechnet rasch $p(0) = p(1) = 1$, $p(2) = 2$, $p(3) = 3$, $p(4) = 5$, $p(5) = 7$, $p(6) = 11$, $p(7) = 15$, $p(8) = 22$, $p(9) = 30$, $p(10) = 42$ usw.

11.4 Das asymptotische Verhalten von $\log p(n)$

Durch Logarithmieren der Partitionenformel von Hardy und Ramanujan aus Bemerkung 1 entsteht $\log p(n) \sim \pi\sqrt{\frac{2n}{3}}$ für $n \to \infty$. Hierfür hat Erdös (1913 - 1986) im Jahre 1941 einen elementaren Beweis geliefert, der 1951 von Newmann zu einem vollständigen Beweis der Hardy-Ramanujanschen Formel ausgebaut wurde. Wir beschränken uns hier auf den Beweis des Ergebnisses von Erdös.

Satz 6. (Erdös) Es gilt

$$\log p(n) \sim \pi\sqrt{\frac{2n}{3}} \qquad (n \to \infty).$$

Der Beweis von Satz 6 beruht entscheidend auf dem folgenden Lemma, das auch von eigenständigem Interesse ist.

Lemma 1. Für $n \in \mathbb{N}$ gilt die Rekursionsformel

$$n\,p(n) = \sum_{\nu k \le n} \nu\, p(n - \nu k) = \sum_{m \le n} \sigma(m)\, p(n-m).$$

Beweis. Werden alle $p(n)$ Partitionen von n addiert, so ergibt sich einerseits die Summe $n\,p(n)$. Andererseits tritt der Summand ν in diesen Partitionen genau $p(n-\nu)+p(n-2\nu)+\cdots$ Male auf. Multiplikation mit ν und Summation über ν ergibt die erste Gleichung. Setzt man darin $\nu\, k = m$ und beachtet $\sigma = 1 * I$, so folgt auch die zweite Gleichung. □

Alternativ kann der Beweis von Lemma 1 auch durch Umformung bekannter Identitäten erbracht werden: Für $|x| < 1$ gilt nämlich wegen Satz 3

$$f(x) = \sum_{n=0}^{\infty} p(n)\, x^n = \prod_{k=1}^{\infty} \frac{1}{1-x^k} = \exp\left(\sum_{k=1}^{\infty} \sum_{\nu=1}^{\infty} \frac{x^{\nu k}}{\nu} \right).$$

Logarithmische Differentiation ergibt

$$\frac{x f'(x)}{f(x)} = \sum_{k=1}^{\infty} \sum_{\nu=1}^{\infty} k\, x^{\nu k} = \sum_{m=1}^{\infty} \sigma(m)\, x^m.$$

Andererseits ist

$$x\,f'(x) = \sum_{n=1}^{\infty} n\,p(n)\,x^n,$$

also

$$\sum_{n=1}^{\infty} n\,p(n)\,x^n = \sum_{\ell=1}^{\infty} p(\ell)\,x^\ell \sum_{m=1}^{\infty} \sigma(m)\,x^m.$$

Ausmultiplikation und Koeffizientenvergleich liefert erneut die Behauptung von Lemma 1.

Es folgt ein technisches Lemma zur asymptotischen Analysis.

Lemma 2. Es sei $a = \pi\sqrt{\frac{2}{3}}$ und $b > 0$. Dann gilt

$$\frac{1}{n} \sum_{m \le n} \sigma(m)\,e^{-b(\sqrt{n}-\sqrt{n-m})} = \frac{a^2}{b^2} + \mathcal{O}(1) \qquad (n \to \infty).$$

Beweis. Für $0 \le y \le 1$ gilt

$$1 \le \frac{2}{1+\sqrt{1-y}} \le \frac{2}{2-y} \le 1 + y.$$

Damit folgt für $1 \le m \le n$

$$\sqrt{n} - \sqrt{n-m} = \frac{m}{2\sqrt{n}}\,\frac{2}{1+\sqrt{1-\frac{m}{n}}} = \frac{m}{2\sqrt{n}} + \vartheta\,m^2 n^{-3/2}$$

mit $0 \le \vartheta = \vartheta(m,n) < 1$. Es entsteht

$$\frac{1}{n} \sum_{m \le n} \sigma(m)\,e^{-b(\sqrt{n}-\sqrt{n-m})} = \frac{1}{n} \sum_{m \le n} \sigma(m)\,e^{-\frac{b}{2\sqrt{n}}\,m}\,e^{-b\,\vartheta m^2 n^{-3/2}} = \frac{1}{n}\,S_1 + \frac{1}{n}\,S_2\,,$$

wobei S_1 die Summe über $1 \le m \le n^{2/3}$ und S_2 die Summe über $n^{2/3} < m \le n$ bezeichnen. Nun ist für $n \to \infty$

$$\frac{1}{n}\,S_2 \le \frac{1}{n} \sum_{n^{2/3} < m \le n} \sigma(m)\,e^{-\frac{b}{2\sqrt{n}}\,m} \le e^{-\frac{b}{2}\,n^{1/6}}\,\frac{1}{n} \sum_{m \le n} \sigma(m) \le n^2\,e^{-\frac{b}{2}\,n^{1/6}} = \mathcal{O}(1),$$

$$\frac{1}{n}\,S_1 = \frac{1}{n} \sum_{m \le n^{2/3}} \sigma(m)\,e^{-\frac{b}{2\sqrt{n}}\,m}\,e^{-b\vartheta m^2 n^{-3/2}} = \big(1 + \mathcal{O}(1)\big)\,\frac{1}{n} \sum_{m \le n^{2/3}} \sigma(m)\,e^{-\frac{b}{2\sqrt{n}}\,m}\,.$$

Partielle Summation mit

$$g(t) = e^{-\frac{b}{2\sqrt{n}}\,t} \quad \text{und} \quad \sum_{m \le t} \sigma(m) = \frac{\zeta(2)}{2}\,t^2 + \mathcal{O}(t^{3/2}) \qquad (t \ge 1)$$

liefert wegen $\zeta(2) = \frac{a^2}{4}$ schließlich

$$\begin{aligned}
&\frac{1}{n} \sum_{m \le n^{2/3}} \sigma(m)\, e^{-\frac{bm}{2\sqrt{n}}} \\
&\qquad = \frac{1}{n}\, e^{-\frac{b}{2} n^{1/6}} \sum_{m \le n^{2/3}} \sigma(m) + \frac{b}{2}\, n^{-3/2} \int_1^{n^{2/3}} \sum_{m \le t} \sigma(m)\, e^{-\frac{b}{2\sqrt{n}} t}\, dt \\
&\qquad = \mathcal{O}(1) + \frac{b\,\zeta(2)}{4}\, n^{-3/2} \int_1^{n^{2/3}} t^2\, e^{-\frac{b}{2\sqrt{n}} t}\, dt + \mathcal{O}\big(n^{-3/2}\big) \int_1^{n^{2/3}} t^{3/2}\, e^{-\frac{b}{2\sqrt{n}} t}\, dt \\
&\qquad = \frac{2\zeta(2)}{b^2} \int_{\frac{b}{2} n^{-1/2}}^{\frac{b}{2} n^{1/6}} x^2 e^{-x}\, dx + \mathcal{O}(1) = \frac{4\zeta(2)}{b^2} + \mathcal{O}(1) = \frac{a^2}{b^2} + \mathcal{O}(1).
\end{aligned}$$

Zusammenfassung ergibt die Behauptung von Lemma 2. □

Nun ist der *Beweis* von Satz 6 rasch erledigt: Für $0 < \varepsilon < 1$ gibt es gemäß Lemma 2 ein $n_0 \in \mathbb{N}$ mit

$$\frac{1}{n} \sum_{m \le n} \sigma(m)\, e^{-(a-\varepsilon)(\sqrt{n}-\sqrt{n-m})} = \Big(\frac{a}{a-\varepsilon}\Big)^2 + \mathcal{O}(1) > 1$$

für alle $n \ge n_0$. Es sei $c_0 = c_0(\varepsilon) > 0$ so gewählt, daß $p(n) e^{-(a-\varepsilon)\sqrt{n}} > c_0$ für alle $n \le n_0$ ausfällt. Das heißt

$$p(n) > c_0\, e^{(a-\varepsilon)\sqrt{n}} \quad \text{für } n \le n_0\,.$$

Wir behaupten

$$p(n) > c_0\, e^{(a-\varepsilon)\sqrt{n}} \quad \text{für alle } n \in \mathbb{N}. \tag{1}$$

Dazu sei $n > n_0$, und $p(\nu) > c_0\, e^{(a-\varepsilon)\sqrt{\nu}}$ gelte schon für alle $\nu < n$. Lemma 1 liefert

$$\begin{aligned}
p(n) &= \frac{1}{n} \sum_{m \le n} \sigma(m)\, p(n-m) > c_0\, \frac{1}{n} \sum_{m \le n} \sigma(m)\, e^{(a-\varepsilon)\sqrt{n-m}} \\
&= c_0\, e^{(a-\varepsilon)\sqrt{n}}\, \frac{1}{n} \sum_{m \le n} \sigma(m)\, e^{-(a-\varepsilon)(\sqrt{n}-\sqrt{n-m})} > c_0\, e^{(a-\varepsilon)\sqrt{n}},
\end{aligned}$$

und (1) folgt nach dem Induktionsprinzip. Ebenso sieht man

$$p(n) < c_1\, e^{(a+\varepsilon)\sqrt{n}} \quad \text{für alle } n \in \mathbb{N} \tag{2}$$

mit einer geeigneten Konstanten $c_1 = c_1(\varepsilon) > 0$. Aus (1) und (2) kommt

$$c_0\, e^{(a-\varepsilon)\sqrt{n}} < p(n) < c_1\, e^{(a+\varepsilon)\sqrt{n}},$$

und Logaritmieren ergibt

$$\Big|\frac{\log p(n)}{\sqrt{n}} - a\Big| \le \varepsilon + \mathcal{O}\Big(\frac{1}{\sqrt{n}}\Big)$$

oder

$$\overline{\lim_{n\to\infty}} \Big|\frac{\log p(n)}{\sqrt{n}} - a\Big| \le \varepsilon$$

für jedes $\varepsilon > 0$. Das heißt $\log p(n) \sim a\sqrt{n}$ für $n \to \infty$, wie in Satz 6 behauptet. □

Bemerkung 3. Die Ungleichung (2) läßt sich leicht zu $p(n) < e^{a\sqrt{n}}$ für alle $n \in \mathbb{N}$ verschärfen. Der Induktionsbeweis beruht allein auf Lemma 1.