

Springer-Lehrbuch

Peter Bundschuh

Einführung in die Zahlentheorie

Sechste, überarbeitete und aktualisierte Auflage

 Springer

Prof. Dr. Peter Bundschuh
Universität Köln
Mathematisches Institut
Weyertal 86–90
50931 Köln

ISBN 978-3-540-76490-8

e-ISBN 978-3-540-76491-5

DOI 10.1007/978-3-540-76491-5

Springer-Lehrbuch ISSN 0937-7433

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Mathematics Subject Classification (2000): 11-01

© 2008, 2002, 1998, 1996, 1992, 1988 Springer-Verlag Berlin Heidelberg

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland vom 9. September 1965 in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtsgesetzes.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürfen.

Satz: Datenerstellung durch den Autor unter Verwendung eines Springer \TeX -Makropakets

Herstellung: LE- \TeX Jelonek, Schmidt & Vöckler GbR, Leipzig

Umschlaggestaltung: WMXDesign GmbH, Heidelberg

Gedruckt auf säurefreiem Papier

9 8 7 6 5 4 3 2 1

springer.de

Vorwort zur Erstaufgabe

Untersuchungen verschiedener Eigenschaften natürlicher Zahlen gehörten historisch zu den ältesten Beschäftigungen mit mathematischen Problemen überhaupt. So entstanden bereits im griechischen Altertum Mathematikbücher wie EUKLIDS *Elemente* und DIOPHANTS *Arithmetika*, die sich teilweise oder ausschließlich mit der systematischen Behandlung ganzzahliger Fragestellungen befaßten. Mit dem ausgehenden Altertum schwand jedoch weitgehend das Interesse an der Mathematik insgesamt und wirklich starke, neue Impulse erhielt die Lehre von den ganzen Zahlen erst wieder im 17. und 18. Jahrhundert, vor allem durch FERMAT und EULER. Während die Nachwelt FERMATs Ergebnisse noch mühsam seiner reichen Korrespondenz mit gebildeten Zeitgenossen entnehmen mußte, publizierte EULER seine Resultate zumeist in Zeitschriftenserien der Akademien, die einige große europäische Höfe eingerichtet hatten.

Die ersten umfassenden und systematischen Darstellungen dessen, was zu ihrer Zeit zum gesicherten Wissen in der Lehre von den ganzen Zahlen gehörte, gaben dann um die Wende zum 19. Jahrhundert nahezu zeitgleich LEGENDRE mit seinem *Essai sur la Théorie des Nombres* (1798) und GAUSS mit seinen *Disquisitiones Arithmeticae* (1801). Vor allem das epochemachende Werk von GAUSS mit seiner Fülle von neuen und tiefliegenden Entdeckungen brachte die Zahlentheorie als selbständige Teildisziplin der Gesamtmathematik erst eigentlich auf den Weg.

In den seither verflossenen fast zweihundert Jahren hat sich die Zahlentheorie gewaltig weiterentwickelt und in verschiedene Richtungen verzweigt. Dementsprechend ist eine umfangreiche zahlentheoretische Literatur entstanden, vom einführenden Lehrbuch bis hin zur speziellen Monographie.

Diese Situation nötigt jedem neu hinzukommenden Autor eine Rechtfertigung für sein Tun ab. So habe ich mir als Ziel gesetzt, die wichtigsten Grundlagen der Zahlentheorie in einer Weise zu präsentieren, die die historische Entwicklung in stärkerem Maße als üblich berücksichtigt. Daneben wollte ich aufzeigen, wie sich bei der Behandlung mancher spezieller Probleme neue Teilgebiete der Zahlentheorie herausgebildet und selbständig weiter entfaltet haben. Davon, daß dieser Prozeß bisweilen in intensiver Wechselwirkung mit anderen mathematischen Disziplinen ablief, zeugen etwa analytische Zahlentheorie und Funktionentheorie. Eine weitere Aufgabe der vorliegenden Darstellung ist die Heranführung des

Lesers an das Studium vertiefender Literatur, die in den Text eingearbeitet und am Ende des Buches zusammengestellt ist.

Behandelt wird in den ersten fünf Kapiteln etwa der Stoff einer einsemestrigen vierstündigen Einführungsvorlesung in die Zahlentheorie. Dabei ergeben sich schon an sehr frühen Stellen neue Probleme, die in späteren Kapiteln wieder aufgegriffen und vertieft werden. So werden z.B. bereits im ersten Kapitel über Teilbarkeit arithmetische bzw. Primzahlfragen angeschnitten, die im fünften und sechsten bzw. siebten fortgeführt werden.

Besonders in den beiden letztgenannten Kapiteln über Transzendenz bzw. Primzahlen soll der Leser beispielhaft lernen, wie die Zahlentheorie sich zur Lösung ihrer Probleme bisweilen anderer mathematischer Disziplinen bedient. Beide Kapitel belegen eindrucksvoll die Leistungsfähigkeit funktionentheoretischer Methoden im Einsatz bei zahlentheoretischen Fragestellungen, wobei im sechsten außerdem einige Sätze aus der Algebra zum benötigten Instrumentarium gehören.

Das Inhaltsverzeichnis gestattet einen sehr detaillierten Überblick über den behandelten Stoff. Dabei wird der eine Kenner dies, der andere jenes vermissen, etwa die Theorie der quadratischen Formen oder die Geometrie der Zahlen, um nur zwei Unterlassungen zu nennen, die in ihrer Gesamtheit von der auferlegten Beschränkung des Buchumfangs herrühren. Aus demselben Grund sind außer kleineren Dingen, die gelegentlich "dem Leser zur Übung überlassen" werden, auch keine Aufgaben eingearbeitet. In dieser Hinsicht muß der interessierte Leser auf einige im Literaturverzeichnis zusammengestellte Bücher verwiesen werden.

Was die Ausführlichkeit der Darstellung angeht, wird sie dem Kenner zu groß sein, während sie dem Anfänger in gewissen Passagen zu knapp erscheinen mag. Generell sollte das Buch, abgesehen von Kap. 1, §§ 5, 6, Kap. 6, §§ 4, 5 und Kap. 7, § 3, jedem interessierten Leser zugänglich sein, der in gymnasialer Oberstufe, universitären Anfängerkursen oder im Selbststudium die Sprache der modernen Mathematik erlernt und eine gewisse Übung im Umgang mit mathematischen Sachverhalten und Schlußweisen erlangt hat.

Ein Zitat 3.4.2 verweist auf Abschnitt 2 im Paragraphen 4 des Kapitels 3, Satz 3.4.2A auf den dort zu findenden Satz A. Innerhalb eines Kapitels bleibt bei Zitaten die Nummer dieses Kapitels weg, im gleichen Paragraphen eines Kapitels auch noch die Paragraphennummer; so wird mit Satz 2A bzw. Lemma 2 der Satz A bzw. das Lemma in Abschnitt 2 desselben Kapitels und Paragraphen zitiert. Schließlich deutet das Zeichen \square das Ende eines Beweises an.

Aus der Reihe der konstruktiven Kritiker, die manche Verbesserung oder Ergänzung angeregt haben, sei Herr Dozent Dr. A. T. PETHÖ besonders hervorgehoben. Nicht zuletzt hat er sich, ebenso wie Herr Dr. S. ECKMANN, der Mühe

unterzogen, die erste Fassung des Manuskripts gewissenhaft durchzusehen; die endgültige Version wurde von Herrn cand. math. T. TÖPFER vollständig geprüft. Allen drei Herren möchte ich für ihre Mithilfe bestens danken. Frau E. STIEHL-SCHÖNDORFER besorgte das Schreibmaschinenmanuskript, Frau E. LORENZ nahm die Erfassung in \TeX vor; beiden Damen gilt mein herzlicher Dank für ihre sorgfältige Arbeit. Schließlich habe ich dem Springer-Verlag für sein Entgegenkommen zu danken.

Köln, im Juli 1987

P. Bundschuh

Vorwort zur zweiten Auflage

Die vorliegende zweite Auflage der “Einführung in die Zahlentheorie” stellt eine korrigierte und, wo nötig, auf den neuesten Stand gebrachte Fassung der 1988 erschienenen Erstauflage dar. Auch das Literaturverzeichnis wurde — dem Geschmack des Verfassers gemäß — aktualisiert, wobei erneut keinerlei Vollständigkeit angestrebt werden konnte.

Danken möchte ich dem Verlag für sein freundliches Angebot, diese Zweitaufgabe meiner “Zahlentheorie” in seine Reihe “Springer-Lehrbuch” aufzunehmen. Schließlich habe ich Herrn Dipl.-Math. R. MÜLLER für die Besorgung der reproduktionsfähigen \TeX -Vorlage der Zweitaufgabe ebenso zu danken wie meinem Sohn RALF, ohne dessen stete Bereitschaft zur Computerunterstützung manche Tabelle nicht so zügig entstanden wäre.

Köln, im Dezember 1991

P. Bundschuh

Vorwort zur dritten Auflage

Gegenüber der zweiten Auflage mußte diese dritte erneut aktualisiert werden, nicht zuletzt wegen des inzwischen gelungenen Beweises der FERMATschen Vermutung. Auch waren einige weitere kleine Inkorrektheiten oder Druckfehler zu beseitigen, auf die ich zum Teil von Lesern der früheren Auflagen hingewiesen wurde, denen ich für ihre Kritik deshalb dankbar bin. Für die technische Herstellung des überarbeiteten Textes danke ich Frau E. STIEHL-SCHÖNDORFER und Herrn Dipl.-Math. B. GREUEL sehr herzlich.

Köln, im Juni 1996

P. Bundschuh

Vorwort zur vierten bis sechsten Auflage

Auch für diese Neuauflagen waren einige Passagen dem aktuellen Stand der Forschung anzupassen, etwa dort, wo Rekorde rasch fallen, wie bei den MERSENNEschen Primzahlen oder bei der Dezimalbruchentwicklung so prominenter Zahlen wie π . Wieder habe ich einer Reihe von Lesern – meine Diktion schließt Leserinnen stets mit ein – für Verbesserungsvorschläge sehr zu danken ebenso wie Frau STIEHL-SCHÖNDORFER und den Herren Dipl.-Math. B. GREUEL und Dr. M. WELTER für ihre Mithilfe bei den jeweiligen Überarbeitungen.

Köln, Juni 1998, März 2002, August 2007

P. Bundschuh

Inhaltsverzeichnis

Kapitel 1. Teilbarkeit	1
§ 1. Fundamentalsatz der Arithmetik	2
1. Natürliche und ganze Zahlen 2. Teiler 3. Primzahlen 4. Satz von EUKLID 5. Der Fundamentalsatz der Arithmetik 6. Kanonische Primfaktorzerlegung 7. Teileranzahl- und Teilersummenfunktion 8. Vollkommene Zahlen 9. Irrationalität 10. Anmerkung zum Eindeutigkeitsbeweis	
§ 2. Größter gemeinsamer Teiler, kleinstes gemeinsames Vielfaches	15
1. Größter gemeinsamer Teiler (ggT) 2. Divisionsalgorithmus 3. Zwei Charakterisierungen des ggT 4. Idealtheoretische Deutung des ggT 5. Rechenregeln 6. Teilerfremdheit 7. Charakterisierung der Primzahlen 8. Nochmals: Eindeutigkeit im Fundamentalsatz 9. Euklidischer Algorithmus und ggT 10. Regelmäßiger Kettenbruch rationaler Zahlen 11. Kleinstes gemeinsames Vielfaches (kgV) 12. Zusammenhang zwischen ggT und kgV	
§ 3. Lineare diophantische Gleichungen	27
1. Warum “diophantisch”? 2. Lösbarkeitsbedingung 3. Der Fall zweier Unbestimmten 4. Spezielle Lösung, numerisches Beispiel 5. Reduktion des allgemeinen Falls 6. Struktur der Lösungsgesamtheit	
§ 4. Zahlentheoretische Funktionen	35
1. Einige Definitionen 2. Multiplikative und additive Funktionen 3. Produktdarstellung unendlicher Reihen 4. RIEMANNsche Zetafunktion 5. Zweimal EUKLIDS Satz 6. Faltung 7. Inverse bezüglich Faltung 8. Die Gruppe der multiplikativen Funktionen 9. MÖBIUSSche Müfunktion 10. Weitere spezielle multiplikative Funktionen 11. EULERS Phifunktion und Verallgemeinerungen 12. Eine Aussage “im Mittel” 13. Wahrscheinlichkeit für Teilerfremdheit 14. Historische Anmerkungen	

§ 5.	Teilbarkeit in Integritätsringen	53
	1. Teiler, Einheiten, Assoziiertheit 2. Die Begriffe ggT und kgV 3. Unzerlegbare Elemente, Primelemente 4. Faktorielle Ringe 5. Hauptidealringe 6. Euklidische Ringe 7. Polynome 8. Polynomringe über Körpern 9. Polynomringe über faktoriellen Ringen	
§ 6.	Algebraische Zahlkörper, insbesondere quadratische	65
	1. Algebraische Zahlen, Minimalpolynom 2. Konjugierte 3. Algebraische Zahlkörper 4. Normen 5. Ganzheit 6. Quadratische Zahlkörper 7. Deren Ganzheitsring 8. Einheiten quadratischer Zahlringe 9. Euklidische quadratische Zahlringe 10. Primzahlen als Summe zweier Quadrate 11. DEDEKINDS Beispiel	
	Kapitel 2. Kongruenzen	78
§ 1.	Lineare Kongruenzen	79
	1. Definition der Kongruenz, elementare Eigenschaften 2. FERMAT-Zahlen 3. Kürzungsregel 4. Vollständige Restsysteme 5. Lineare Kongruenzen 6. Bruchschreibweise 7. Restklassenring 8. Prime Restklassengruppe 9. Historische Bemerkungen	
§ 2.	Simultane lineare Kongruenzen	88
	1. Reduktion des Problems 2. Paarweise teilerfremde Moduln 3. Anwendungen, numerische Beispiele 4. Restklassenring als direkte Summe 5. Prime Restklassengruppe als direktes Produkt 6. Historische Bemerkungen	
§ 3.	Die Sätze von Fermat, Euler und Wilson	94
	1. DIRICHLETS Schubfachprinzip 2. Kongruenzverhalten von Potenzen 3. Der “kleine” FERMATSche Satz 4. Der EULERSche Satz 5. Numerische Anwendungen 6. Zusammengesetzt oder Primzahl? 7. FERMAT–EULER und geheime Nachrichtenübermittlung 8. Satz von WILSON 9. Anwendung auf eine quadratische Kongruenz	
§ 4.	Polynomiale Kongruenzen	104
	1. Problemstellung 2. Reduktion auf Primzahlpotenzmoduln 3. Überlegungen zur weiteren Reduktion 4. Reduktion auf Primzahlmoduln 5. Polynomkongruenzen bei Primzahlmoduln 6. Ein Beispiel	

§ 5.	Primitivwurzeln	109
	1. Definition 2. Primitivwurzeln modulo Primzahlen 3. Tabellen für Primitivwurzeln 4. Zu welchen Moduln sind Primitivwurzeln möglich? 5. Bestimmung aller Moduln mit Primitivwurzeln 6. Zweierpotenzen als Moduln 7. Basisdarstellung	

Kapitel 3. Potenzreste, insbesondere quadratische Reste 121

§ 1.	Indexrechnung und Potenzreste	121
	1. Indizes 2. Ein Beispiel 3. n -te Potenzreste, quadratische Reste und Nichtreste 4. Kriterium für n -te Potenzreste 5. Folgerungen aus dem Kriterium 6. n -te Potenzreste, Modulzerlegung in Primzahlpotenzen	
§ 2.	Quadratische Reste	127
	1. Quadratische Kongruenzen und quadratische Reste 2. Kriterium für quadratische Reste 3. Das LEGENDRE-Symbol 4. EULERS Kriterium 5. GAUSSSches Lemma 6. Quadratisches Reziprozitätsgesetz, Ergänzungssätze 7. Beweis des Reziprozitätsgesetzes 8. Ein numerisches Beispiel 9. Quadratische Nichtreste modulo Primzahlen 10. Primzahlen in arithmetischen Progressionen 11. Primfaktoren von FERMAT-Zahlen 12. MERSENNE-Primzahlen 13. Historisches zum Reziprozitätsgesetz	
§ 3.	Verteilung quadratischer Reste	147
	1. Summen über gewisse LEGENDRE-Symbole 2. Paare sukzessiver quadratischer Reste 3. Tripel sukzessiver quadratischer Reste 4. Eigenschaften JACOBSTHALScher Summen	

Kapitel 4. Additive Probleme und diophantische Gleichungen .. 153

§ 1.	Potenzsummen, insbesondere Quadratsummen	154
	1. Primzahlen als Summe zweier Quadrate 2. THUES Lemma 3. Natürliche Zahlen als Summe zweier Quadrate 4. Natürliche Zahlen als Summe von vier Quadraten: LAGRANGES Satz 5. Nochmals Primzahlen als Summe zweier Quadrate 6. Summen dreier Quadrate 7. WARINGS Problem und HILBERTS Satz 8. Anmerkungen über Darstellungsanzahlen	

§ 2.	Polynomiale diophantische Gleichungen	167
	1. Pythagoräische Tripel 2. EUKLIDS Satz über pythagoräische Tripel	
	3. Rationale Punkte auf Kurven zweiten Grades 4. Rationale Punkte	
	gewisser Kurven dritten Grades 5. Resultate von POINCARÉ, MORDELL	
	und FALTINGS 6. Pythagoräische Dreiecke quadratischer Kathetenlängen	
	7. FERMATS Vermutung 8. Weitere Entwicklung des FERMAT-Problems	
	(bis 1993) 9. Lösung des FERMAT-Problems	
§ 3.	Die Pellsche Gleichung und Verwandtes	185
	1. Problemstellung 2. Der DIRICHLETSche Approximationssatz 3. Un-	
	endlich viele Lösungen der PELL-Gleichung 4. Lösungsstruktur der	
	PELL-Gleichung 5. Pythagoräische Dreiecke mit Kathetendifferenz Eins	
	6. Einheiten reell-quadratischer Zahlkörper 7. Ganze Punkte auf Kur-	
	ven zweiten Grades 8. Anmerkungen dazu	
	Kapitel 5. Verschiedene Entwicklungen reeller Zahlen	200
§ 1.	Die g-adische Entwicklung	201
	1. Entwicklung natürlicher Zahlen 2. Teilbarkeitsregeln 3. Der gebro-	
	chene Teil reeller Zahlen 4. Entwicklung reeller Zahlen 5. Entwicklung	
	rationaler Zahlen 6. Periodizitätseigenschaften der Ziffernfolge 7. Dezi-	
	malbruchentwicklungen 8. Rationale Zahlen mit gleichen Nennern 9. Ei-	
	ne Anwendung des Irrationalitätskriteriums 10. Existenz transzendenter	
	Zahlen 11. Dezimalbruchentwicklung und Dichtung 12. Historische An-	
	merkungen	
§ 2.	Die Cantorsche Entwicklung. Weitere	
	Irrationalitätskriterien	216
	1. Beschreibung der Entwicklung 2. CANTORSche Reihen und Irratio-	
	nalität 3. Verwandte Irrationalitätskriterien 4. Anwendungen	
§ 3.	Die regelmäßige Kettenbruchentwicklung	222
	1. Der Kettenbruchalgorithmus 2. Konvergenz unendlicher Kettenbrü-	
	che 3. Eindeutigkeit, Irrationalität 4. Periodische Kettenbrüche 5. Der	
	Satz von LAGRANGE 6. Zur Minimallösung der PELLschen Gleichung	
	7. Annäherung reeller Zahlen durch rationale 8. Beste Näherungen	
	9. Anmerkungen dazu 10. Approximation algebraischer Zahlen zwei-	
	ten Grades durch rationale 11. Eine arithmetische Eigenschaft von $e^{2/k}$	
	12. Kettenbruchentwicklung von e	

Kapitel 6. Transzendenz	242
§ 1. Entdeckung der Transzendenz	242
1. Historisches 2. Der LIOUVILLESche Approximationssatz 3. Konstruktion transzendenter Kettenbrüche 4. Transzendente g -adische Reihen	
§ 2. Schärfere Approximationssätze	248
1. Der THUE-SIEGEL-ROTHsche Satz 2. Anwendungen auf Transzendenz 3. THUE-Gleichung und ROTHs Verallgemeinerung 4. Reduktion auf den THUE-SIEGEL-ROTHschen Satz 5. Effektivitätsfragen 6. SCHMIDTs Sätze über simultane Approximation	
§ 3. Die Sätze von Hermite, Lindemann und Weierstraß	257
1. Historisches 2. Hauptergebnisse von HERMITE und LINDEMANN 3. Der Satz von LINDEMANN-WEIERSTRASS 4. Zur Äquivalenz der vier Versionen	
§ 4. Die Methode von Hermite-Mahler	263
1. Vorbemerkungen 2. Ungleichungen für algebraische Zahlen 3. Konstruktion geeigneter Exponentialpolynome 4. Eigenschaften dieser Exponentialpolynome 5. Eine Determinantenbetrachtung 6. Gewinnung einer nichtverschwindenden algebraischen Zahl 7. Untere Abschätzung 8. Obere Abschätzung 9. Parameterwahl 10. Historische Anmerkung	
§ 5. Der Satz von Gel'fond-Schneider	271
1. HILBERTs siebtes Problem 2. Ein Schubfachschluß 3. SIEGELSches Lemma 4. Hilfsfunktion für GEL'FOND-SCHNEIDER 5. Gewinnung einer zur Abschätzung geeigneten Zahl 6. Untere Abschätzung 7. Obere Abschätzung 8. Parameterwahl 9. Ausblicke	
Kapitel 7. Primzahlen	282
§ 1. Elementare Ergebnisse	282
1. Darstellung von Primzahlen durch Polynome 2. Exponentielle Folgen von Primzahlen 3. Große Lücken 4. Sieb des ERATOSTHENES, Primzahltafeln 5. Anzahlfunktion 6. Primzahlzwillinge 7. Die GOLDBACH-Probleme	

§ 2.	Anzahlfunktion: Tchebycheffs Sätze	293
	1. Vermutungen von LEGENDRE und GAUSS 2. LEGENDRES Identität	
	3. Obere Abschätzung 4. Partielle Summation 5. Zwei asymptotische	
	Ergebnisse von MERTENS 6. Letzte Vorstufe des Primzahlsatzes	
§ 3.	Der Primzahlsatz	301
	1. RIEMANNS Anstoß 2. Konvergenz einer Folge und Primzahlsatz	
	3. Die Reste der Zetareihe 4. Fortsetzung und Nullstellenfreiheit der	
	RIEMANNSchen Zetafunktion 5. Über gewisse DIRICHLET-Reihen 6. Die	
	Existenz des Grenzwerts 7. Anwendung des CAUCHY-Kriteriums	
	8. Konvergenzsatz 9. Mittelwert der MÖBIUS-Funktion 10. Funktio-	
	nalgleichung der Zetafunktion 11. Pole und Nullstellen der Zetafunktion	
	12. RIEMANNSche Vermutung 13. Schlußbemerkungen	
	Literaturverzeichnis	324
	Namen- und Sachverzeichnis	328