Vorwort

Das vorliegende Buch entstand aus dem Skript zur Vorlesung „Elementare Zahlentheorie“, die ich im Sommersemester 2017 an der Universität zu Köln gehalten habe. Diese richtete sich vorwiegend an Bachelor-Studierende mit Fachrichtung Mathematik bzw. Lehramt Mathematik im 4. bis 6. Fachsemester.

Der behandelte Stoff entspricht im Wesentlichen den Themenkomplexen, die üblicherweise in einer einsemestrigen Vorlesung zur Elementaren Zahlentheorie behandelt werden: Im ersten Kapitel wird die grundlegende Teilbarkeitstheorie in den ganzen Zahlen untersucht, insbesondere der Euklidische Algorithmus und der größte gemeinsame Teiler, elementare Primzahlverteilung und zahlentheoretische Funktionen. Im zweiten Kapitel geht es dann um modulare Arithmetik und Kongruenzen. Als Anwendungen hierzu stellen wir unter anderem einige einfache Primzahltests sowie kryptographische Verfahren, insbesondere das RSA-Verfahren, vor. Das Hauptresultat des dritten Kapitels ist das quadratische Reziprozitätsgesetz, eines der zentralen Resultate der gesamten Zahlentheorie, und einige seiner Anwendungen. Im vierten Kapitel geht es dann um Diophantische Gleichungen, speziell pythagoreische Tripel und Spezialfälle des Letzten Satzes von Fermat, sowie Summen von Quadratzahlen. Im fünften Kapitel werden mit g-adischen Darstellungen bzw. Kettenbrüchen zwei verschiedene Möglichkeiten zur Darstellung und Approximation reeller Zahlen vorgestellt. Im sechsten und letzten Kapitel wird eine kurze Einführung in die Theorie der quadratischen Formen gegeben

mit besonderem Augenmerk auf binäre quadratische Formen und ihre Reduktionstheorie und einem Beweis des Drei-Quadrate-Satzes.

Ein wichtiger Aspekt in der Zahlentheorie ist, dass man vieles explizit ausrechnen kann. Deswegen werden im Laufe des Buches, wo es möglich ist, Beweise algorithmisch geführt und Rechenverfahren explizit vorgestellt. Zur Einübung finden sich am Ende der meisten Abschnitte Übungsaufgaben, die den Stoff weiter vertiefen sollen und mit einigen Rechenverfahren vertraut machen sollen. Um auch das Selbststudium zu erleichtern, werden im Anhang zur Kontrolle die Lösungen der Rechenaufgaben und zu ausgewählten weiteren Aufgaben Hinweise zur Lösung angegeben.

Es soll noch darauf hingewiesen werden, dass dieses vorliegende Buch natürlich nicht das einzige zum Thema elementare Zahlentheorie ist. In Teilen orientiert es sich vor allem an folgenden Lehrbüchern, die ich auch zur weiteren Lektüre empfehlen möchte:

- P. Bundschuh, *Einführung in die Zahlentheorie*, 6. Auflage, Springer-Verlag, 2008.

- H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics **138**, 4. Auflage, Springer-Verlag, 2000. (insbesondere zu Kapitel 6)

- R. Remmert und P. Ullrich, *Elementare Zahlentheorie*, 3. Auflage, Birkhäuser-Verlag, 2008.

- D. Zagier, *Zetafunktionen und quadratische Körper*, Springer-Verlag, 1981. (insbesondere zu Kapitel 6)

Neben der Elementaren Zahlentheorie, die sich im Wesentlichen mit Eigenschaften der ganzen Zahlen beschäftigt und in der Regel nur auf Methoden aus den Grundvorlesungen zurückgreift, unterteilt man die Zahlentheorie noch in zwei weitere Bereiche, die allerdings ineinandergreifen und nicht strikt voneinander abzugrenzen sind. Dies sind einerseits die Analytische Zahlentheorie, die zahlentheoretische

Fragen, wie z.B. nach dem Wachstum zahlentheoretischer Funktionen (vgl. Abschnitt 1.4) oder der Verteilung der Primzahlen, mittels analytischer und insbesondere auch funktionentheoretischer Methoden untersucht. Andererseits hat man noch die Algebraische Zahlentheorie, die unter anderem danach fragt, wie sich Konzepte wie die Primfaktorzerlegung in den ganzen Zahlen auf etwa Erweiterungen derselben in sogenannten *algebraischen Zahlkörpern* verallgemeinern lassen. Einführende Texte in die Zahlentheorie, die auch auf Aspekte der Analytischen und Algebraischen Zahlentheorie eingehen, sind zum Beispiel

- G. H. Hardy und E. M. Wright, *An Introduction to the Theory of Numbers*, 6. Auflage, Oxford University Press, 2009.
- Hua L.-K., *Introduction to Number Theory*, Springer-Verlag, 1982.
- K. Ireland und M. Rosen, *A Classical Introduction to Modern Number Theory*, 2. Auflage, Springer-Verlag, 1990.

Die Liste der zu empfehlenden Bücher zur weiteren Lektüre ließe sich noch nahezu beliebig lange fortsetzen. Weitere Lehrbücher und auch Originalarbeiten werden im Laufe des Buches zitiert und finden sich in der Literaturliste im Anhang.

Mein ganz besonderer Dank gilt Claudia Alfes-Neumann, Adrian Hauffe-Waschbüsch, Martin Raum, Sebastian Schönnenbeck, Markus Schwagenscheidt, Annalena Wernz und José-Miguel Zapata-Rolón, die Teile des Manuskriptes durchgesehen haben und durch zahlreiche Korrekturen und Vorschläge maßgeblich zu dessen Verbesserung beigetragen haben. Für ihre Hilfe bei der Gestaltung des Umschlagbildes danke ich Iris Wirker. Zum Schluss möchte ich noch dem Verlag für sein Entgegenkommen danken.

Köln, im Februar 2019, Michael H. Mertens

Einführung

Warum Zahlentheorie?

Die (elementare) Zahlentheorie kann sicherlich neben der Geometrie als eines der ältesten Teilgebiete der Mathematik überhaupt angesehen werden. Anders als die Geometrie, die u. a. aus Anwendungen z.B. bei der Vermessung von Ländereien entstanden ist, taucht sie allerdings zuerst als reine Geistesübung, die bei den Pythagoräern sogar den Status der Religion erreichte, auf. Eine der wichtigsten Sammlungen des Wissens um die Zahlentheorie in der griechischen Antike sind sicherlich die *Elemente* von EUKLID. Dort werden z.B. die Natur von Primzahlen und Teilbarkeit natürlicher Zahlen studiert, mit der wir uns auch zu Beginn dieses Buches beschäftigen wollen (siehe Kapitel 1). Später untersuchte DIOPHANTUS die nach ihm benannten DIOPHANTischen Gleichungen, die uns in Kapitel 4 begegnen werden und heute ein wichtiges und bis heute extrem aktives Teilgebiet der Mathematik bilden.

Was einen großen Teil der Faszination an der Zahlentheorie ausmacht, ist sicherlich die Tatsache, dass viele Problemstellungen in ihr sehr einfach zu formulieren sind, aber sehr schwer, z.T. bis heute überhaupt nicht, zu lösen sind. Einige Beispiele sind die folgenden, auf die wir teilweise im Laufe der Vorlesung noch näher zu sprechen kommen.

Vollkommene Zahlen Eine (natürliche) Zahl heißt *vollkommen*, wenn sie gleich der Summe ihrer echten Teiler (also aller Teiler außer sich selbst) ist. Die kleinste vollkommene Zahl ist $6 = 1 + 2 + 3$. Seit der Antike sind die vier vollkommenen Zahlen 6, 28, 496 und 8128 bekannt, die nächstgrößere, 33 550 336, wurde erst 1536 von dem deutschen Rechenmeister Ulrich Rieger veröffentlicht [Reg36]. Euler konnte die geraden vollkommenen Zahlen vollständig charakterisieren [Eul49]. Bis heute ist aber zum Beispiel weder bekannt, ob es unendlich viele vollkommene Zahlen gibt, noch ob es auch nur eine einzige ungerade vollkommene Zahl gibt. In Abschnitt 1.4 werden wir uns näher mit diem Problem der vollkommenen Zahlen beschäftigen.

Heron**-Zahlen** Der Flächeninhalt eines rechtwinkligen Dreieckes mit Katheten a und b ist bekanntlich $\frac{1}{2}ab$. Nach dem Satz des Pythagoras ist die Länge der Hypothenuse c genau $c = \sqrt{a^2 + b^2}$. Gibt man nun eine natürliche Zahl n für den Flächeninhalt eines solchen Dreieckes vor, so lassen sich offensichtlich unendlich viele rationale Zahlen a und b finden, so dass $\frac{1}{2}ab = n$ gilt, allerdings wird in aller Regel die Hypothenuse c keine rationale Länge haben. Man nennt n eine Heron-*Zahl* (manchmal auch *Dreieckszahl*, im Englischen *congruent number*), falls es doch eine Wahl rationaler a und b gibt, so dass auch c rational ist. Zum Beispiel ist $n = 6$ eine Heron-Zahl, da das Dreieck mit Seitenlängen $a = 3$, $b = 4$, $c = 5$ rechtwinklig ist und den Flächeninhalt $\frac{1}{2} \cdot 3 \cdot 4 = 6$ hat. Das Tripel $(3, 4, 5)$ nennt man ein *Pythagoreisches Tripel*, d.h. ein Tripel ganzer Zahlen (a, b, c), die die Beziehung $a^2 + b^2 = c^2$ erfüllen. Diese werden in Abschnitt 4.1 näher untersucht. Für ein solches Pythagoreisches Tripel ist $n = \frac{1}{2}ab$ eine Heron-Zahl. Es gibt allerdings auch Heron-Zahlen, die nicht von solchen Tripeln herkommen, z.B. ist 5 kongruent, wie man durch das Dreieck mit Seitenlängen $a = \frac{3}{2}$, $b = \frac{20}{3}$, $c = \frac{41}{6}$ sieht. Wie sich herausstellt, ist die Frage, ob eine gegebene Zahl n eine Heron-Zahl ist oder nicht, nach derzeitigem Wissensstand [Tun83] im Allgemeinen nur unter Zuhilfenahme der sogenannten Birch und Swinnerton-Dyer-Vermutung zu beantworten, obwohl das Problem seit der Anti-

ke untersucht wird. Der Beweis dieser Vermutung ist eines der sieben sogenannten Millenniumsprobleme des Clay Mathematics Instituts [Wil06] und damit eines der wahrscheinlich wichtigsten offenen Probleme der modernen Mathematik. In der Tat gilt das Problem der HERON-Zahlen neben dem Problem der vollkommenen Zahlen als das letzte ungelöste Problem der klassischen Antike.

Primzahlverteilung Primzahlen und ihre Verteilung üben seit jeher eine besondere Faszination auf Zahlentheoretiker aus. Einerseits bilden sie einen fundamental wichtigen Baustein der ganzen Zahlen (man vergleicht sie gern mit Atomen, die die ganzen Zahlen aufbauen), andererseits scheint ihr Auftreten in der Folge der natürlichen Zahlen im Wesentlichen chaotisch. Dieses scheinbare Chaos zu ordnen ist eine der Hauptaufgaben in der Zahlentheorie. Manche Fragen über Primzahlen sind recht leicht zu beantworten, z. B. dass es unendlich viele davon gibt, andere sind schon komplizierter, aber noch elementar lösbar, so z. B. die Tatsache, dass die Summe $\sum_{p \text{ prim}} \frac{1}{p}$ divergiert, oder das BERTRANDsche Postulat, dass es für jede natürliche Zahl n zwischen n und $2n$ stets eine Primzahl gibt. In Abschnitt 1.3 werden wir uns ausführlicher mit diesen Fragen befassen. Mit Hilfsmitteln aus der Funktionentheorie, die über das zur Verfügung stehende Instrumentarium dieses Buches deutlich hinausgehen, lässt sich der große Primzahlsatz beweisen, der eine überraschend einfache Näherung für die Anzahl der Primzahlen unterhalb einer gegebenen Schranke angibt. Andere Fragen wiederum sind seit langer Zeit und bis heute völlig offen, z. B. ob es stehts zwischen zwei aufeinander folgenden Quadratzahlen stets 2 Primzahlen gibt [Opp82], oder ob es unendlich viele *Primzahl-Zwillinge* gibt, d.h. Paare $(p, p+2)$, wo p und $p+2$ beides Primzahlen sind. Seit dem Jahr 2013 weiß man immerhin, dass es unendlich oft vorkommt, dass zwei aufeinanderfolgende Primzahlen sich um höchstens 70 000 000 unterscheiden [Zha14]. Diese Schranke ist in der Tat inzwischen auf 246 gesunken [May15, Pol14], aber für tatsächliche Primzahl-Zwillinge reichen die heute verfügbaren Methoden nicht aus.

FERMATs letzter Satz Bereits weiter oben sind uns Pythaogoreische Tripel begegnet, d.h. ganzzahlige Lösungen der Gleichung $a^2 + b^2 = c^2$. Wir werden in Kapitel 4 zeigen, dass es unendlich viele ganze Zahlen (a, b, c) gibt, die diese Gleichung erfüllen und diese parametrisieren. FERMAT betrachtete nun im 17. Jahrhundert bereits die folgende Verallgemeinerung der Pythagoreischen Gleichung,

$$a^n + b^n = c^n, \qquad n \geq 2$$

In seiner Ausgabe von DIOPHANTUS *Arithmetika* schrieb FERMAT als Randnotiz, er habe „einen wahrhaft wundervollen Beweis gefunden“, dass diese Gleichung in den ganzen Zahlen für $n \geq 3$ keine Lösung hat, nur sei „jener Rand nicht breit genug ihn zu fassen“. Diese Aussage ist als der Letzte oder Große Satz von FERMAT bekannt geworden und stellte Mathematiker für fast 350 Jahre vor ein scheinbar unlösbares Rätsel. Viele große Mathematiker der folgenden Jahrhunderte, wie etwa EULER, LEGENDRE, GERMAIN , KUMMER, KRONECKER, HILBERT und viele, viele andere mehr konnten zwar verschiedene Spezialfälle von FERMATs letztem Satz beweisen, seinen „wahrhaft wundervollen Beweis“ aber fand niemand. Ein Beweis ließ bis 1995 auf sich warten, als WILES unter Aufbringung des gesamten Wissens der modernen Algebraischen Zahlentheorie endlich FERMATs letzten Satz beweisen konnte [Wil95, TW95]. Angesichts der Komplexität von WILES Beweis, der sich über mehrere 100 Seiten erstreckt, gilt es inzwischen als ausgeschlossen, dass FERMAT seinen letzten Satz tatsächlich beweisen konnte. Wir werden in diesem Buch nicht wirklich auf dieses Thema eingehen können, Interessierten möchte ich daher das (allgemeinverständliche) Buch [Sin00] empfehlen. FERMATs letzter Satz wird in einigen Spezialfällen in Abschnitt 4.1 behandelt.

Neben der rein mathematischen Faszination ist die Zahlentheorie auch aus unserem Alltagsleben kaum noch wegzudenken. Moderne Kryptographie, ohne die unsere heutige digitalisierte Welt nicht vor-

stellbar ist, basiert fast immer auf zahlentheoretischen Überlegungen. In der Kryptographie möchte man natürlich, dass eine zu sendende Nachricht möglichst leicht zu *ver*schlüsseln und mit dem richtigen Schlüssel auch leicht zu *ent*schlüsseln ist, ohne den richtigen Schlüssel aber möglichst nicht oder nur sehr schwer zu entschlüsseln ist. Man verwendet hierfür oft den Begriff der *trapdoor*-Funktion. Davon gibt es in der Zahlentheorie zahlreiche Beispiele. Ein naives solches ist die Primfaktorzerlegung. So ist es sehr leicht, Zahlen praktisch beliebiger Größe zu multiplizieren, aber eine „große“ Zahl in ihre Primfaktoren zu zerlegen, ist im Allgemeinen sehr schwierig. Z.B. wird niemand große Schwierigkeiten darin sehen, das Produkt

$$193\,707\,721 \cdot 761\,838\,257\,287 = 147\,573\,952\,589\,676\,412\,927 = 2^{67} - 1$$

zu berechnen, die Aufgabe, diese Faktoren zu finden kostete aber nach seinen eigenen Angaben Frank Nelson Cole die Sonntage von drei Jahren [Col04] (warum er gerade diese Faktorisierung bestimmt hat, werden wir später sehen). Einer der Grundgedanken hinter einem immer noch standardmäßigen Verschlüsselungsverfahren, dem RSA-Verfahren, ist genau dieser, dass die Faktorisierung großer Zahlen sehr schwer ist. Der eigentliche mathematische Kern des Verfahrens aber ist der sogenannte kleine Satz von Fermat, der, vor fast 350 Jahren im Prinzip um seiner selbst Willen gefunden, nun die Grundlage unserer heutigen Kommunikation liefert. Eine ausführlichere Diskussion hierzu findet sich in Abschnitt 2.4.

Grundlagen über ganze Zahlen

Leopold Kronecker hat einmal gesagt [Web92]

> Die ganzen Zahlen hat der liebe Gott gemacht, alles Andere ist Menschenwerk.

Für diese Vorlesung werden wir Kroneckers These insoweit folgen, dass wir die ganzen (bzw. natürlichen) Zahlen und ihre elementaren

Eigenschaften als gegeben annehmen wollen und sie nicht erst etwa aus den Axiomen der Mengenlehre herleiten. Der Vollständigkeit halber deuten wir hier nun die wichtigsten dieser Eigenschaften an. Hier und im Folgenden schreiben wir stets

$$\mathbb{N} = \{1, 2, 3, ...\}$$

für die Menge der *natürlichen Zahlen* und

$$\mathbb{Z} = \{0, \pm 1, \pm 2, ...\}$$

für die Menge der *ganzen Zahlen*. Gelegentlich verwenden wir auch

$$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$$

sowie die Bezeichnungen $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ für die Mengen der *rationalen*, *reellen*, bzw. *komplexen Zahlen*.

Die natürlichen Zahlen können wie folgt charakterisiert werden. Die Menge $\mathbb{N}$ enthält ein ausgezeichnetes Element 1 und es gibt eine injektive Selbstabbildung $S : \mathbb{N} \to \mathbb{N}$ mit $1 \notin S(\mathbb{N})$ und der Eigenschaft, dass für jede Teilmenge $M \subseteq \mathbb{N}$ mit $1 \in M$ und $S(M) \subseteq M$ bereits $M = \mathbb{N}$ gilt. Man nennt diese Eigenschaft das *Induktionsprinzip*, dass die formale Grundlage für die Beweismethode der vollständigen Induktion bildet.

Mittels dieses Prinzips kann man zeigen, dass die altvertrauten Rechenoperationen $+$ und $\cdot$ den üblichen Rechenregeln gehorchen (Kommutativgesetz, Assoziativgesetz, Distributivgesetz). Bezüglich der Addition bilden die natürlichen Zahlen damit eine (kommutative) *Halbgruppe*, bezüglich der Multiplikation ein kommutatives *Monoid*, da das Element 1 das neutrale Element der Multiplikation ist ($n \cdot 1 = n$ für alle $n \in \mathbb{N}$). Weiters kann man auf $\mathbb{N}$ die natürliche Relation $\leq$ mit der bekannten Bedeutung und den üblichen Variationen $<, \geq, >$ erklären, die mit den Rechenoperationen verträglich ist. Eine wichtige Eigenschaft von $\mathbb{N}$ ist der so genannte *Wohlordnungssatz*: Bezüglich der Ordnung $\leq$ besitzt jede nicht-leere Teilmenge von $\mathbb{N}$ ein kleinstes