A Comprehensive Course in Number Theory

Developed from the author's popular text, *A Concise Introduction to the Theory of Numbers*, this book provides a comprehensive initiation to all the major branches of number theory. Beginning with the rudiments of the subject, the author proceeds to more advanced topics, including elements of cryptography and primality testing; an account of number fields in the classical vein including properties of their units, ideals and ideal classes; aspects of analytic number theory including studies of the Riemann zeta-function, the prime-number theorem and primes in arithmetical progressions; a description of the Hardy–Littlewood and sieve methods from, respectively, additive and multiplicative number theory; and an exposition of the arithmetic of elliptic curves.

The book includes many worked examples, exercises and, as with the earlier volume, there is a guide to further reading at the end of each chapter. Its wide coverage and versatility make this book suitable for courses extending from the elementary to the graduate level.

Alan Baker, FRS, is Emeritus Professor of Pure Mathematics in the University of Cambridge and Fellow of Trinity College, Cambridge. His many distinctions include the Fields Medal (1970) and the Adams Prize (1972).

A COMPREHENSIVE COURSE IN NUMBER THEORY

ALAN BAKER
University of Cambridge

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town,
Singapore, São Paulo, Delhi, Mexico City

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9781107019010

First published 2012

Printed in the United Kingdom at the University Press, Cambridge

A catalogue record for this publication is available from the British Library

Library of Congress Cataloguing in Publication data
Baker, Alan, 1939–
A comprehensive course in number theory / Alan Baker.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-107-01901-0 (hardback)
1. Number theory – Textbooks. I. Title.
QA241.B237 2012
512.7–dc23
2012013414

ISBN 978-1-107-01901-0 Hardback
ISBN 978-1-107-60379-0 Paperback

Contents

Cambridge University Press
978-1-107-01901-0 - A Comprehensive Course in Number Theory
Alan Baker
Frontmatter
More information

Preface

This is a sequel to my earlier book, *A Concise Introduction to the Theory of Numbers*. The latter was based on a short preparatory course of the kind traditionally taught in Cambridge at around the time of publication about 25 years ago. Clearly it was in need of updating, and it was originally intended that a second edition be produced. However, on looking through, it became apparent that the work would blend well with more advanced material arising from my lecture courses in Cambridge at a higher level, and it was decided accordingly that it would be more appropriate to produce a substantially new book. The now much expanded text covers elements of cryptography and primality testing. It also provides an account of number fields in the classical vein including properties of their units, ideals and ideal classes. In addition it covers various aspects of analytic number theory including studies of the Riemann zeta-function, the prime-number theorem, primes in arithmetical progressions and a brief exposition of the Hardy–Littlewood and sieve methods. Many worked examples are given and, as with the earlier volume, there are guides to further reading at the ends of the chapters.

The following remarks, taken from the *Concise Introduction*, apply even more appropriately here:

> The theory of numbers has a long and distinguished history, and indeed the concepts and problems relating to the field have been instrumental in the foundation of a large part of mathematics. It is very much to be hoped that our exposition will serve to stimulate the reader to delve into the rich literature associated with the subject and thereby to discover some of the deep and beautiful theories that have been created as a result of numerous researches over the centuries. By way of introduction, there is a short account of the *Disquisitiones Arithmeticae* of Gauss, and, to begin with, the reader can scarcely do better than to consult this famous work.

To complete the text there is a chapter on elliptic curves; here my main source has been lecture notes by Dr Tom Fisher of a course that he has given regularly in Cambridge in recent times. I am indebted to him for generously providing me with a copy of the notes and for further expert advice. I am grateful also to Mrs Michèle Bailey for her invaluable secretarial assistance with my lectures over many years and to Dr David Tranah of Cambridge University Press for his constant encouragement in the production of this book.

Cambridge 2012 A.B.

Introduction

Gauss and Number Theory†

Without doubt the theory of numbers was Gauss' favourite subject. Indeed, in a much quoted dictum, he asserted that Mathematics is the Queen of the Sciences and the Theory of Numbers is the Queen of Mathematics. Moreover, in the introduction to Eisenstein's *Mathematische Abhandlungen*, Gauss wrote:

> The Higher Arithmetic presents us with an inexhaustible storehouse of interesting truths – of truths, too, which are not isolated but stand in the closest relation to one another, and between which, with each successive advance of the science, we continually discover new and sometimes wholly unexpected points of contact. A great part of the theories of Arithmetic derive an additional charm from the peculiarity that we easily arrive by induction at important propositions which have the stamp of simplicity upon them but the demonstration of which lies so deep as not to be discovered until after many fruitless efforts; and even then it is obtained by some tedious and artificial process while the simpler methods of proof long remain hidden from us.

All this is well illustrated by what is perhaps Gauss' most profound publication, namely his *Disquisitiones Arithmeticae*. It has been described, quite justifiably I believe, as the Magna Carta of Number Theory, and the depth and originality of thought manifest in this work are particularly remarkable considering that it was written when Gauss was only about 18 years of age. Of course, as Gauss said himself, not all of the subject matter was new at the time of writing, and Gauss acknowledged the considerable debt that he owed to earlier scholars, in particular Fermat, Euler, Lagrange and Legendre. But the *Disquisitiones Arithmeticae* was the first systematic treatise on the Higher Arithmetic and it provided the foundations and stimulus for a great volume

† This article was originally prepared for a meeting of the British Society for the History of Mathematics held in Cambridge in 1977 to celebrate the bicentenary of Gauss' birth.

of subsequent research which is in fact continuing to this day. The importance of the work was recognized as soon as it was published in 1801 and the first edition quickly became unobtainable; indeed many scholars of the time had to resort to taking handwritten copies. But it was generally regarded as a rather impenetrable work and it was probably not widely understood; perhaps the formal Latin style contributed in this respect. Now, however, after numerous reformulations, most of the material is very well known, and the earlier sections at least are included in every basic course on number theory.

The text begins with the definition of a congruence, namely two numbers are said to be congruent modulo n if their difference is divisible by n. This is plainly an equivalence relation in the now familiar terminology. Gauss proceeds to the discussion of linear congruences and shows that they can in fact be treated somewhat analogously to linear equations. He then turns his attention to power residues and introduces, amongst other things, the concepts of primitive roots and indices; and he notes, in particular, the resemblance between the latter and the ordinary logarithms. There follows an exposition of the theory of quadratic congruences, and it is here that we meet, more especially, the famous law of quadratic reciprocity; this asserts that if p, q are primes, not both congruent to 3 (mod 4), then p is a residue or non-residue of q according as q is a residue or non-residue of p, while in the remaining case the opposite occurs. As is well known, Gauss spent a great deal of time on this result and gave several demonstrations; and it has subsequently stimulated much excellent research. In particular, following works of Jacobi, Eisenstein and Kummer, Hilbert raised as the ninth of his famous list of problems presented at the Paris Congress of 1900 the question of obtaining higher reciprocity laws, and this led to the celebrated studies of Furtwängler, Artin and others in the context of class field theory.

By far the largest section of the *Disquisitiones Arithmeticae* is concerned with the theory of binary quadratic forms. Here Gauss describes how quadratic forms with a given discriminant can be divided into classes so that two forms belong to the same class if and only if there exists an integral unimodular substitution relating them, and how the classes can be divided into genera, so that two forms are in the same genus if and only if they are rationally equivalent. He proceeds to apply these concepts so as, for instance, to throw light on the difficult question of the representation of integers by binary forms. It is a remarkable and beautiful theory with many important ramifications. Indeed, after re-interpretation in terms of quadratic fields, it became apparent that it could be applied much more widely, and in fact it can be regarded as having provided the foundations for the whole of algebraic number theory. The term 'Gaussian field', meaning the field generated over the rationals by i, is a reminder of Gauss' pioneering work in this area.

The remainder of the *Disquisitiones Arithmeticae* contains results of a more miscellaneous character, relating, for instance, to the construction of 17-sided polygons, which was clearly of particular appeal to Gauss, and to what is now termed the cyclotomic field, that is, the field generated by a primitive root of unity. And especially noteworthy here is the discussion of certain sums involving roots of unity, now referred to as Gaussian sums, which play a fundamental role in the analytic theory of numbers.

I conclude this introduction with some words of Mordell. In an essay published in 1917 he wrote 'The theory of numbers is unrivalled for the number and variety of its results and for the beauty and wealth of its demonstrations. The Higher Arithmetic seems to include most of the romance of mathematics. As Gauss wrote to Sophie Germain, the enchanting beauties of this sublime study are revealed in their full charm only to those who have the courage to pursue it.' And Mordell added 'We are reminded of the folk-tales, current amongst all peoples, of the Prince Charming who can assume his proper form as a handsome prince only because of the devotedness of the faithful heroine.'