Lecture Notes in Mathematics 2171

More information about this series at http://www.springer.com/series/304

Steve Wright

Quadratic Residues and Non-Residues

Selected Topics

Springer

Steve Wright
Department of Mathematics and Statistics
Oakland University
Rochester
Michigan, U.S.A.

ISSN 0075-8434 ISSN 1617-9692 (electronic)
Lecture Notes in Mathematics
ISBN 978-3-319-45954-7 ISBN 978-3-319-45955-4 (eBook)
DOI 10.1007/978-3-319-45955-4

Library of Congress Control Number: 2016956697

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

For Linda

Preface

Although number theory as a coherent mathematical subject started with the work of Fermat in the 1630s, modern number theory, i.e., the systematic and mathematically rigorous development of the subject from fundamental properties of the integers, began in 1801 with the appearance of Gauss' landmark treatise *Disquisitiones Arithmeticae* [19]. A major part of the *Disquisitiones* deals with quadratic residues and non-residues: if p is an odd prime, an integer z is a quadratic residue (respectively, a quadratic non-residue) of p if there is (respectively, is not) an integer x such that $x^2 \equiv z \mod p$. As we shall see, quadratic residues arise naturally as soon as one wants to solve the general quadratic congruence $ax^2 + bx + c \equiv 0 \mod m$, $a \not\equiv 0 \mod m$, and this, in fact, motivated some of the interest which Gauss himself had in them. Beginning with Gauss' fundamental contributions, the study of quadratic residues and non-residues has subsequently led directly to many of the key ideas and techniques that are used everywhere in number theory today, and the primary goal of these lecture notes is to use this study as a window through which to view the development of some of those ideas and techniques. In pursuit of that goal, we will employ methods from elementary, analytic, and combinatorial number theory as well as methods from the theory of algebraic numbers.

In order to follow these lectures most profitably, the reader should have some familiarity with the basic results of elementary number theory. An excellent source for this material (and much more) is the text [30] of Kenneth Ireland and Michael Rosen, *A Classical Introduction to Modern Number Theory*. A feature of this text that is of particular relevance to what we discuss is Ireland and Rosen's treatment of quadratic and higher-power residues, which is noteworthy for its elegance and completeness as well as for its historical perspicacity. We will in fact make use of some of their work in Chaps. 3 and 7.

Although not absolutely necessary, some knowledge of algebraic number theory will also be helpful for reading these notes. We will provide complete proofs of some facts about algebraic numbers and we will quote other facts

without proof. Our reference for proof of the latter results is the classical treatise of Erich Hecke [27], *Vorlesungen über die Theorie der Algebraischen Zahlen*, in the very readable English translation by G. Brauer and J. Goldman. About Hecke's text André Weil [58, foreword] had this to say: "To improve upon Hecke, in a treatment along classical lines of the theory of algebraic numbers, would be a futile and impossible task." We concur enthusiastically with Weil's assessment and highly recommend Hecke's book to all those who are interested in number theory.

We next offer a brief overview of what is to follow. The notes are arranged in a series of ten chapters. Chapter 1, an introduction to the subsequent chapters, provides some motivation for the study of quadratic residues and non-residues by consideration of what needs to be done when one wishes to solve the general quadratic congruence mentioned above. We briefly discuss the contents of the *Disquisitiones Arithmeticae*, present some biographical information about Gauss, and also record some basic results from elementary number theory that will be used frequently in the sequel. Chapter 2 provides some useful facts about quadratic residues and non-residues upon which the rest of the chapters are based. Here we also describe a procedure which provides a strategy for solving what we call the *Basic Problem*: if d is an integer, find all primes p such that d is a quadratic residue of p. The Law of Quadratic Reciprocity is the subject of Chap. 3. We present seven proofs of this fundamentally important result (five in Chap. 3, one in Chap. 7, and one in Chap. 8), which focus primarily (but not exclusively) on the ideas used in the proofs of quadratic reciprocity which Gauss discovered. Chapter 4 discusses some interesting and important applications of quadratic reciprocity, having to do with the solution of the Basic Problem from Chap. 2 and with the structure of the finite subsets S of the positive integers possessing at least one of the following two properties: for infinitely many primes p, S is a set of quadratic residues of p, or for infinitely many primes p, S is a set of quadratic non-residues of p. Here the fundamental contributions of Dirichlet to the theory of quadratic residues enter our story and begin a major theme that will play throughout the rest of our work. Chapter 4 concludes with an interesting application of quadratic residues in modern cryptology, to so-called zero-knowledge or minimal-disclosure proofs. The use of transcendental methods in the theory of quadratic residues, begun in Chap. 4, continues in Chap. 5 with the study of the zeta function of an algebraic number field and its application to the solution of some of the problems taken up in Chap. 4. Chapter 6 gives elementary proofs of some of the results in Chap. 5 which obviate the use made there of the zeta function. The question of how quadratic residues and non-residues of a prime p are distributed among the integers $1, 2, \ldots, p-1$ is considered in Chap. 7, and there we highlight additional results and methods due to Dirichlet which employ the basic theory of L-functions attached to Dirichlet characters determined by certain moduli. Because of the importance that positivity of the values at $s = 1$ of Dirichlet L-functions plays in the proof of the results

of Chap. 7, we present in Chap. 8 a discussion and proof of Dirichlet's class-number formula as a way to definitively explain why the values at $s = 1$ of L-functions are positive. In Chap. 9 the occurrence of quadratic residues and non-residues as arbitrarily long arithmetic progressions is studied by means of some ideas of Harold Davenport [5] and some techniques in combinatorial number theory developed in recent work of the author [62, 63]. A key issue that arises in our approach to this problem is the estimation of certain character sums over the field of p elements, p a prime, and we address this issue by using some results of Weil [57] and Perel'muter [44]. Our discussion concludes with Chap. 10, where the Central Limit Theorem from the theory of probability and a theorem of Davenport and Paul Erdös [7] are used to provide evidence for the contention that as the prime p tends to infinity, quadratic residues of p are distributed randomly throughout certain subintervals of the set $\{1, 2, \ldots, p-1\}$.

These notes are an elaboration of the contents of a special-topics-in-mathematics course that was offered during the summer semesters of 2014 and 2015 at Oakland University. I am very grateful to my colleague Meir Shillor for suggesting that I give such a course and for thereby providing me with the impetus to think about what such a course would entail. I am also very grateful to my colleagues Eddie Cheng and Serge Kruk, the former for giving me very generous and valuable assistance with numerous LaTeX issues which arose during the preparation of the manuscript and the latter for formatting all of the figures in the text. I thank my students Saad Al Najjar, Amelia McIlvenna, and Julian Venegas for reading an early version of the notes and offering several insightful comments which were very helpful to me. My sincere and heartfelt appreciation is also tendered to the anonymous referees for many comments and suggestions which resulted in a very substantial improvement in both the content and exposition of these notes. Finally, and above all others, I am grateful beyond words to my dear wife Linda for her unstinting love, support, and encouragement; this humble missive is dedicated to her.

Rochester, MI, USA Steve Wright

Contents