

Lecture Notes in Mathematics

2171

Editors-in-Chief:

J.-M. Morel, Cachan

B. Teissier, Paris

Advisory Board:

Camillo De Lellis, Zurich

Mario di Bernardo, Bristol

Michel Brion, Grenoble

Alessio Figalli, Zurich

Davar Khoshnevisan, Salt Lake City

Ioannis Kontoyiannis, Athens

Gabor Lugosi, Barcelona

Mark Podolskij, Aarhus

Sylvia Serfaty, New York

Anna Wienhard, Heidelberg

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

© Springer International Publishing Switzerland 2016

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

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 $x^2 \equiv z \pmod{p}$. As we shall see, quadratic residues arise naturally as soon as one wants to solve the general quadratic congruence $ax^2 + bx + c \equiv 0 \pmod{m}$, $a \not\equiv 0 \pmod{m}$, 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 $1, 2, \dots, p - 1$ 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 Erdős [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 $\{1, 2, \dots, p - 1\}$.

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

1	Introduction: Solving the General Quadratic Congruence Modulo a Prime	1
1.1	Linear and Quadratic Congruences	1
1.2	The <i>Disquisitiones Arithmeticae</i>	5
1.3	Notation, Terminology, and Some Useful Elementary Number Theory	6
2	Basic Facts	9
2.1	The Legendre Symbol, Euler's Criterion, and Other Important Things	9
2.2	The Basic Problem and the Fundamental Problem for a Prime	13
2.3	Gauss' Lemma and the Fundamental Problem for the Prime 2.....	16
3	Gauss' <i>Theorema Aureum</i>: The Law of Quadratic Reciprocity	21
3.1	What is a Reciprocity Law?	22
3.2	The Law of Quadratic Reciprocity	25
3.3	Some History	28
3.4	Proofs of the Law of Quadratic Reciprocity	33
3.5	A Proof of Quadratic Reciprocity via Gauss' Lemma	34
3.6	Another Proof of Quadratic Reciprocity via Gauss' Lemma	38
3.7	A Proof of Quadratic Reciprocity via Gauss Sums: Introduction	40
3.8	Algebraic Number Theory	41
3.9	Proof of Quadratic Reciprocity via Gauss Sums: Conclusion	49
3.10	A Proof of Quadratic Reciprocity via Ideal Theory: Introduction	55
3.11	The Structure of Ideals in a Quadratic Number Field	56

- 3.12 Proof of Quadratic Reciprocity via Ideal Theory: Conclusion 64
- 3.13 A Proof of Quadratic Reciprocity via Galois Theory 72
- 4 Four Interesting Applications of Quadratic Reciprocity 79**
 - 4.1 Solution of the Fundamental Problem for Odd Primes 80
 - 4.2 Solution of the Basic Problem 83
 - 4.3 Sets of Integers Which Are Quadratic Residues of Infinitely Many Primes 88
 - 4.4 Intermezzo: Dirichlet’s Theorem on Primes in Arithmetic Progression 91
 - 4.5 The Asymptotic Density of Primes 97
 - 4.6 The Density of Primes Which Have a Given Finite Set of Quadratic Residues 98
 - 4.7 Zero-Knowledge Proofs and Quadratic Residues 107
 - 4.8 Jacobi Symbols 110
 - 4.9 An Algorithm for Fast Computation of Legendre Symbols 113
- 5 The Zeta Function of an Algebraic Number Field and Some Applications 119**
 - 5.1 Dedekind’s Ideal Distribution Theorem 120
 - 5.2 The Zeta Function of an Algebraic Number Field 129
 - 5.3 The Zeta Function of a Quadratic Number Field 137
 - 5.4 Proof of Theorem 4.12 and Related Results 139
 - 5.5 Proof of the Fundamental Theorem of Ideal Theory 146
- 6 Elementary Proofs 151**
 - 6.1 Whither Elementary Proofs in Number Theory? 151
 - 6.2 An Elementary Proof of Theorem 5.13 152
 - 6.3 An Elementary Proof of Theorem 4.12 158
- 7 Dirichlet *L*-Functions and the Distribution of Quadratic Residues 161**
 - 7.1 Positivity of Sums of Values of a Legendre Symbol 162
 - 7.2 Proof of Theorem 7.1: Outline of the Argument 165
 - 7.3 Some Useful Facts About Dirichlet *L*-Functions 166
 - 7.4 Calculation of a Gauss Sum 169
 - 7.5 Some Useful Facts About Analytic Functions of a Complex Variable 173
 - 7.6 The Convergence of Fourier Series 176
 - 7.7 Proof of Theorems 7.2, 7.3, and 7.4 182

7.8	An Elegant Proof of Lemma 4.8 for Real Dirichlet Characters.....	192
7.9	A Proof of Quadratic Reciprocity via Finite Fourier Series	196
8	Dirichlet’s Class-Number Formula	203
8.1	Some Structure Theory for Dirichlet Characters	204
8.2	The Structure of Real Primitive Dirichlet Characters	205
8.3	Elements of the Theory of Quadratic Forms	208
8.4	Representation of Integers by Quadratic Forms and the Class Number.....	209
8.5	The Class-Number Formula.....	212
8.6	The Class-Number Formula and the Class Number of Quadratic Fields	220
8.7	A Character-Theoretic Proof of Quadratic Reciprocity	223
9	Quadratic Residues and Non-Residues in Arithmetic Progression	227
9.1	Long Sets of Consecutive Residues and Non-Residues	228
9.2	Long Sets of Residues and Non-Residues in Arithmetic Progression.....	230
9.3	Weil Sums and Their Estimation.....	232
9.4	Solution of Problems 1 and 3	238
9.5	Solution of Problems 2 and 4: Introduction	242
9.6	Preliminary Estimate of $q_\varepsilon(p)$	244
9.7	Calculation of $\Sigma_4(p)$: Preliminaries	247
9.8	The (B, \mathbf{S}) -Signature of a Prime	249
9.9	Calculation of $\Sigma_4(p)$: Conclusion	251
9.10	Solution of Problems 2 and 4: Conclusion	254
9.11	An Interesting Class of Examples	258
9.12	The Asymptotic Density of $\Pi_+(\mathbf{a}, \mathbf{b})$	269
10	Are Quadratic Residues Randomly Distributed?	273
10.1	Irregularity of the Distribution of Quadratic Residues	273
10.2	Detecting Random Behavior Using the Central Limit Theorem.....	275
10.3	Verifying Random Behavior via a Result of Davenport and Erdős	277
	Bibliography	285
	Index	289