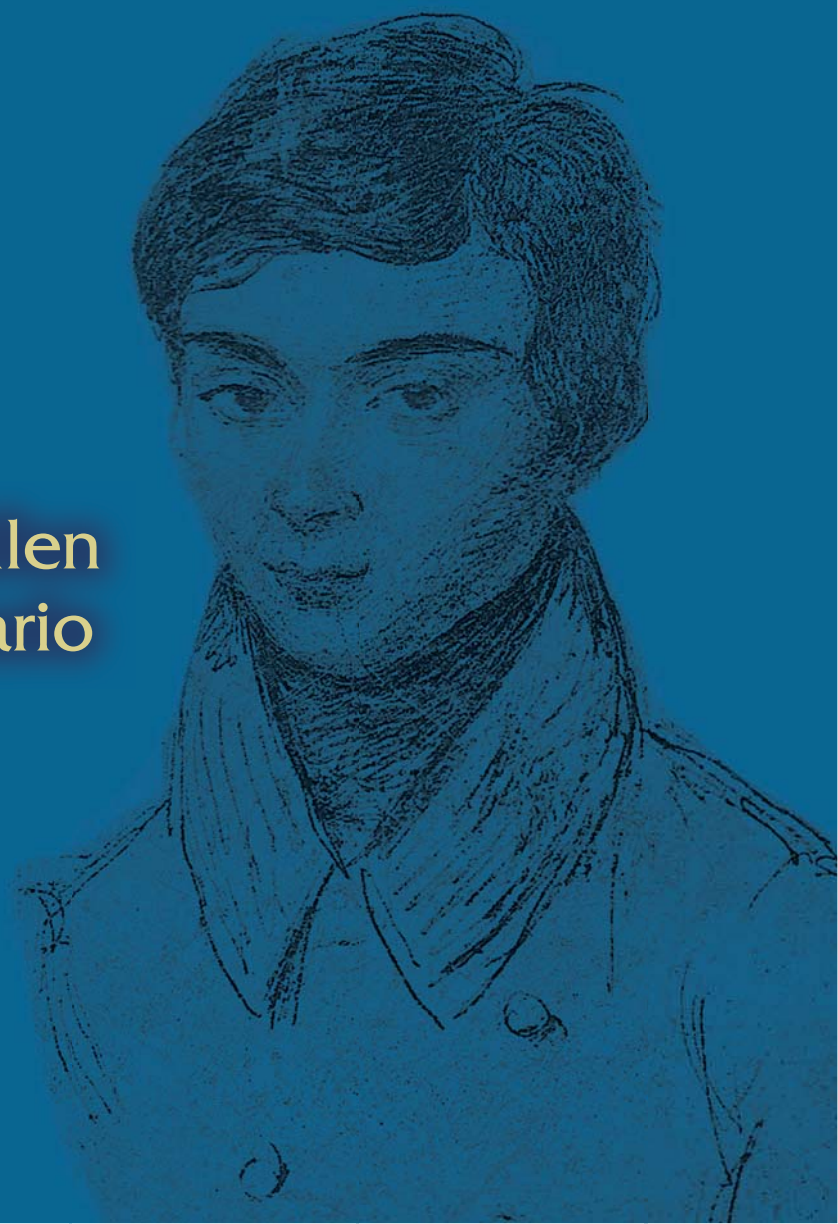
DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor KENNETH H. ROSEN

HANDBOOK OF FINITE FIELDS



Gary L. Mullen
Daniel Panario

CRC Press
Taylor & Francis Group

A CHAPMAN & HALL BOOK

HANDBOOK OF FINITE FIELDS

DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor
Kenneth H. Rosen, Ph.D.

R. B. J. T. Allenby and Alan Slomson, How to Count: An Introduction to Combinatorics, Third Edition

Craig P. Bauer, Secret History: The Story of Cryptology

Juergen Bierbrauer, Introduction to Coding Theory

Katalin Bimbó, Combinatory Logic: Pure, Applied and Typed

Donald Bindner and Martin Erickson, A Student's Guide to the Study, Practice, and Tools of Modern Mathematics

Francine Blanchet-Sadri, Algorithmic Combinatorics on Partial Words

Miklós Bóna, Combinatorics of Permutations, Second Edition

Richard A. Brualdi and Dragoš Cvetković, A Combinatorial Approach to Matrix Theory and Its Applications

Kun-Mao Chao and Bang Ye Wu, Spanning Trees and Optimization Problems

Charalambos A. Charalambides, Enumerative Combinatorics

Gary Chartrand and Ping Zhang, Chromatic Graph Theory

Henri Cohen, Gerhard Frey, et al., Handbook of Elliptic and Hyperelliptic Curve Cryptography

Charles J. Colbourn and Jeffrey H. Dinitz, Handbook of Combinatorial Designs, Second Edition

Abhijit Das, Computational Number Theory

Martin Erickson, Pearls of Discrete Mathematics

Martin Erickson and Anthony Vazzana, Introduction to Number Theory

Steven Furino, Ying Miao, and Jianxing Yin, Frames and Resolvable Designs: Uses, Constructions, and Existence

Mark S. Gockenbach, Finite-Dimensional Linear Algebra

Randy Goldberg and Lance Riek, A Practical Handbook of Speech Coders

Jacob E. Goodman and Joseph O'Rourke, Handbook of Discrete and Computational Geometry, Second Edition

Titles (continued)

Jonathan L. Gross, Combinatorial Methods with Computer Applications

Jonathan L. Gross and Jay Yellen, Graph Theory and Its Applications, Second Edition

Jonathan L. Gross and Jay Yellen, Handbook of Graph Theory

David S. Gunderson, Handbook of Mathematical Induction: Theory and Applications

Richard Hammack, Wilfried Imrich, and Sandi Klavžar, Handbook of Product Graphs, Second Edition

Darrel R. Hankerson, Greg A. Harris, and Peter D. Johnson, Introduction to Information Theory and Data Compression, Second Edition

Darel W. Hardy, Fred Richman, and Carol L. Walker, Applied Algebra: Codes, Ciphers, and Discrete Algorithms, Second Edition

Daryl D. Harms, Miroslav Kraetzl, Charles J. Colbourn, and John S. Devitt, Network Reliability: Experiments with a Symbolic Algebra Environment

Silvia Heubach and Toufik Mansour, Combinatorics of Compositions and Words

Leslie Hogben, Handbook of Linear Algebra

Derek F. Holt with Bettina Eick and Eamonn A. O'Brien, Handbook of Computational Group Theory

David M. Jackson and Terry I. Visentin, An Atlas of Smaller Maps in Orientable and Nonorientable Surfaces

Richard E. Klima, Neil P. Sigmon, and Ernest L. Stitzinger, Applications of Abstract Algebra with Maple™ and MATLAB®, Second Edition

Richard E. Klima and Neil P. Sigmon, Cryptology: Classical and Modern with Maplets

Patrick Knupp and Kambiz Salari, Verification of Computer Codes in Computational Science and Engineering

William Kocay and Donald L. Kreher, Graphs, Algorithms, and Optimization

Donald L. Kreher and Douglas R. Stinson, Combinatorial Algorithms: Generation Enumeration and Search

Hang T. Lau, A Java Library of Graph Algorithms and Optimization

C. C. Lindner and C. A. Rodger, Design Theory, Second Edition

San Ling, Huaxiong Wang, and Chaoping Xing, Algebraic Curves in Cryptography

Nicholas A. Loehr, Bijective Combinatorics

Toufik Mansour, Combinatorics of Set Partitions

Alasdair McAndrew, Introduction to Cryptography with Open-Source Software

Elliott Mendelson, Introduction to Mathematical Logic, Fifth Edition

Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, Handbook of Applied Cryptography

Stig F. Mjølsnes, A Multidisciplinary Introduction to Information Security

Jason J. Molitierno, Applications of Combinatorial Matrix Theory to Laplacian Matrices of Graphs

Titles (continued)

Richard A. Mollin, Advanced Number Theory with Applications

Richard A. Mollin, Algebraic Number Theory, Second Edition

Richard A. Mollin, Codes: The Guide to Secrecy from Ancient to Modern Times

Richard A. Mollin, Fundamental Number Theory with Applications, Second Edition

Richard A. Mollin, An Introduction to Cryptography, Second Edition

Richard A. Mollin, Quadratics

Richard A. Mollin, RSA and Public-Key Cryptography

Carlos J. Moreno and Samuel S. Wagstaff, Jr., Sums of Squares of Integers

Gary L. Mullen and Daniel Panario, Handbook of Finite Fields

Goutam Paul and Subhamoy Maitra, RC4 Stream Cipher and Its Variants

Dingyi Pei, Authentication Codes and Combinatorial Designs

Kenneth H. Rosen, Handbook of Discrete and Combinatorial Mathematics

Douglas R. Shier and K.T. Wallenius, Applied Mathematical Modeling: A Multidisciplinary Approach

Alexander Stanoyevitch, Introduction to Cryptography with Mathematical Foundations and Computer Implementations

Jörn Steuding, Diophantine Analysis

Douglas R. Stinson, Cryptography: Theory and Practice, Third Edition

Roberto Togneri and Christopher J. deSilva, Fundamentals of Information Theory and Coding Design

W. D. Wallis, Introduction to Combinatorial Designs, Second Edition

W. D. Wallis and J. C. George, Introduction to Combinatorics

Jiacun Wang, Handbook of Finite State Based Models and Applications

Lawrence C. Washington, Elliptic Curves: Number Theory and Cryptography, Second Edition

DISCRETE MATHEMATICS AND ITS APPLICATIONS

Series Editor KENNETH H. ROSEN

HANDBOOK OF FINITE FIELDS

Gary L. Mullen
Daniel Panario

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

A CHAPMAN & HALL BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20130515

International Standard Book Number-13: 978-1-4398-7382-3 (eBook - PDF)

To Bevie Sue, with love,
Gary L. Mullen

Para Lucia, Natan, Diego y Lucas
por todo lo vivido juntos... y por lo que vendrá.
Daniel Panario

This page intentionally left blank

Contents

Part I: Introduction

Part II: Theoretical Properties

Part III: Applications

Preface

The CRC Handbook of Finite Fields (hereafter referred to as the *Handbook*) is a reference book for the theory and applications of finite fields. It is not intended to be an introductory textbook. Our goal is to compile in one volume the state of the art in research in finite fields and their applications. Hence, our aim is a comprehensive book, with easy-to-access references for up-to-date facts and results regarding finite fields.

The *Handbook* is organized into three parts. Part I contains just one chapter which is devoted to the history of finite fields through the 18-th and 19-th centuries.

Part II contains theoretical properties of finite fields. This part of the *Handbook* contains 12 chapters. Chapter 2 deals with basic properties of finite fields; properties that are used in various places throughout the entire *Handbook*. Near the end of Section 2.1 is a rather extensive list of recent finite field-related books; these books include textbooks, books dealing with theoretical topics as well as books dealing with various applications to such topics as combinatorics, algebraic coding theory for the error-free transmission of information, and cryptography for the secure transmission of information. Also included is a list of recent finite field-related conference proceedings volumes.

Chapter 2 also provides rather extensive tables of polynomials useful when dealing with finite field computational issues. The website `http://www.crcpress.com/product/isbn/9781439873786` provides larger and more extensive versions of the tables presented in Section 2.2.

The next two chapters deal with polynomials such as irreducible and primitive polynomials over finite fields. Chapter 5 discusses various kinds of bases over finite fields, and Chapter 6 discusses character and exponential sums over finite fields.

In Chapter 7, results on solutions of equations over finite fields are discussed. Chapter 8 covers permutation polynomials in one and several variables, as well as a discussion of value sets of polynomials, and exceptional polynomials over finite fields. Chapter 9 discusses special functions over finite fields. This discussion includes Boolean, APN, PN, bent, kappa polynomials, planar functions and Dickson polynomials, and finishes with a discussion of Schur's conjecture.

Sequences over finite fields are considered in Chapter 10. This chapter includes material on finite field transforms, LFSRs and maximal length sequences, correlation and autocorrelation and linear complexity of sequences as well as algebraic dynamical systems over finite fields.

Chapter 11 deals with various kinds of finite field algorithms including basic finite field computational techniques, formulas for polynomial counting, irreducible techniques, factorizations of polynomials in one and several variables, discrete logarithms, and standard models for finite fields.

In Chapter 12, curves over finite fields are discussed in great detail. This discussion includes elliptic and hyperelliptic curves. Rational points on curves are considered as well as towers and zeta functions over finite fields. In addition, there is a discussion of p-adic estimates of zeta and L-functions over finite fields.

Chapter 13 discusses a variety of topics over finite fields. These topics include relations between the integers and polynomials over finite fields, matrices over finite fields, linear algebra and related computational topics, as well as classical groups over finite fields, and Carlitz and Drinfeld modules.

Part III of the *Handbook*, containing four chapters, discusses various important applications, including mathematical as well as very practical applications of finite fields. Latin

squares and the polynomial method, useful in various areas of combinatorics, are considered. In addition, affine and projective planes, projective spaces, block designs, and difference sets are discussed in detail. In each of these areas, since these topics contain an immense number of papers, we discuss only those techniques and topics related to finite fields. Other topics included in Chaper 14 are (t, m, s)-nets useful in numerical integration, applications of primitive polynomials over finite fields, and Ramanujan and expander graphs.

Chapter 15 is another important chapter in the *Handbook*. It discusses algebraic coding theory and includes a long introductory section dealing with basics properties of codes. This is followed by sections on special kinds of codes including LDPC codes, turbo codes, algebraic geometry codes, raptor codes, and polar codes.

Chapter 16 deals with cryptographic systems over finite fields. In the first section various basic issues dealing with cryptography are discussed. Next to be discussed are stream and block ciphers, multivariate cryptographic systems, elliptic and hyperelliptic curve cryptographic systems as well as systems arising from Abelian varieties over finite fields.

Finally, in Chapter 17 we discuss several additional applications of finite fields including finite fields in biology, quantum information theory, and various applications in engineering including topics like optimal orthogonal codes, binary sequences with small aperiodic autocorrelation, and sequences with small Hamming correlation.

In the bibliography, we have included for each reference, the pages where that reference is discussed in the *Handbook*. There is also a large index to help readers quickly locate various topics in the *Handbook*.

The *Handbook* is not meant to be read in a sequential way. Instead, each section is meant to be self-contained. Basic properties of finite fields are included in Chapter 2. Proofs are not included in the *Handbook*; instead authors have given references where proofs of the important results can be found. In an effort to help the reader locate proofs and important results for each section, at the end of each section we have provided a list of references used in that section. Those reference numbers refer to the main bibliography at the end of the *Handbook* which contains over 3,000 references. A short "See also" section is included for most sections; these are intended to provide the reader with references to other related sections and references of the *Handbook*.

The following numbering system is in effect in the *Handbook*. Within a given section, all results, theorems, corollaries, definitions, examples, etc., are numbered consecutively (with the exception of tables and figures). For example, the result numbered 2.1.5 happens to be a theorem which is the fifth listing in Section 2.1 of Chapter 2. We have also included many remarks in each section. These are also numbered as part of the same system so that for example, Remark 2.1.4 is the fourth listing in Section 2.1.

Readers are encouraged to make us aware of corrections to the material presented here. Readers should contact the author(s) of the section involved, as well as both of the Editors-in-Chief.

We would of course like to first thank the authors of the various sections for their time and effort. Without their help, the *Handbook* would, quite simply, not exist. We also greatly appreciate the authors' willingness to use our style and format so that the entire *Handbook* has a consistent and uniform style and format. While we appreciate the help of all of the authors, we would especially like to thank Ian Blake, Steve Cohen, Cary Huffman, Alfred Menezes, Harald Niederreiter, Henning Stichtenoth, and Arne Winterhof who not only wrote several sections, but who also provided the Editors-in-Chief with valuable input in numerous aspects of the *Handbook*. Every section was reviewed by at least two external reviewers, in addition to the Editors-in-Chief. We also would like to thank the many reviewers who took the time to read and send us comments on the various sections and drafts. Without their help, we would of course have ended up with a volume of considerably diminished quality. We would like to thank Brett Stevens and David Thomson for their help with various

LaTeX and file issues. Finally, we would like to thank Shashi Kumar for his invaluable help in setting up, reworking, and running the style files that define the overall look of the entire Handbook. His efforts were of tremendous help to us. We would also like to thank Bob Stern for his continued support.

Needless to say, this project has involved many, many hours. We thank Bevie Sue Mullen and Lucia Moura for their encouragement, support, love, and patience during the entire process.

Gary L. Mullen
Daniel Panario

This page intentionally left blank

Editors-in-Chief

Gary L. Mullen
Department of Mathematics
The Pennsylvania State University
University Park, PA 16802
U.S.A.
Email: mullen@math.psu.edu

Daniel Panario
School of Mathematics and Statistics
Carleton University
Ottawa ON K1S 5B6
Canada
Email: daniel@math.carleton.ca

Contributors

Omran Ahmadi
School of Mathematics
Institute for Research in Fundamental Sciences (IPM)
P. O. Box: 19395-5746, Tehran
Iran
Email: oahmadid@ipm.ir

Simeon Ball
Departament Matematica Aplicada IV
Universitat Politecnica Catalunya
c/Jordi Girona 1-3
08034 Barcelona
Spain
Email: simeon@ma4.upc.edu

Daniel J. Bernstein
Department of Computer Science (MC 152)
University of Illinois at Chicago
851 S. Morgan Street
Chicago, IL 60607-7053
U.S.A
Email: djb@cr.yp.to

Régis Blache
IUFM de Guadeloupe
Morne Ferret
97139 Les Abymes
French West Indies
Email: rblache@iufm.univ-ag.fr

Ian F. Blake
Department of Electrical and Computer Engineering
University of British Columbia
Vancouver, BC V6T 1Z4
Canada
Email: ifblake@ece.ubc.ca

Aart Blokhuis
Department of Mathematics and Computer Science
Eindhoven University of Technology
P.O. Box 513
5600 MB
The Netherlands
Email: aartb@win.tue.nl

Claude Carlet
University of Paris 8
Department of Mathematics
2 rue de la Liberté
93526 Saint-Denis, Cedex
France
Email: claude.carlet@univ-paris8.fr

Francis Castro
Department of Mathematics
University of Puerto Rico
Rio Piedras Campus
San Juan, 00931
Puerto Rico
Email: franciscastr@gmail.com

Pascale Charpin
INRIA-Rocquencourt
Domaine de Voluceau, B.P. 105
F-78153 Le Chesnay Cedex
France
Email: Pascale.Charpin@inria.fr

Sebastian M. Cioabă
Department of Mathematical Sciences
University of Delaware
Newark, DE 19716-2553
U.S.A.
Email: cioaba@math.udel.edu

Stephen D. Cohen
School of Mathematics & Statistics
University of Glasgow
Glasgow G12 8QW
Scotland
Email: Stephen.Cohen@glasgow.ac.uk

Charles J. Colbourn
School of CIDSE
Arizona State University
Tempe, AZ 85287-8809
U.S.A.
Email: Charles.Colbourn@asu.edu

Robert Coulter
Department of Mathematical Sciences
University of Delaware
520 Ewing Hall
Newark, DE 19716
U.S.A.
Email: coulter@math.udel.edu

Jintai Ding
Department of Mathematical Sciences
University of Cincinnati
2815 Commons Way
Cincinnati, OH 45221-0025
U.S.A.
Email: jintai.ding@gmail.com

Jeff Dinitz
Department of Mathematics and Statistics
University of Vermont
Burlington, VT 05405
U.S.A.
Email: Jeff.Dinitz@uvm.edu

Christophe Doche
Department of Computing
Macquarie University
North Ryde, NSW 2109
Australia
Email: christophe.doche@mq.edu.au

Jean-Guillaume Dumas
Université Joseph Fourier, Grenoble I
Laboratoire Jean Kuntzmann
Mathématiques Appliquées et Informatique
38041 Grenoble
France
Email: Jean-Guillaume.Dumas@imag.fr

Gary Ebert
N3691 Sylvan Isle Drive
Watersmeet, MI 49969
U.S.A.
Email: ebert@math.udel.edu

Gove Effinger
Department of Mathematics and Computer Science
Skidmore College
Saratoga Springs, NY 12866
U.S.A.
Email: effinger@skidmore.edu

Andreas Enge
INRIA Bordeaux - Sud-Ouest
Université Bordeaux 1
351 cours de la Libération
33405 Talence Cedex
France
Email: andreas.enge@inria.fr

Ron Evans
Department of Mathematics
University of California at San Diego
La Jolla, CA 92093-0112
U.S.A.
Email: revans@ucsd.edu

Haining Fan
School of Software
Tsinghua University
Beijing
China
Email: fhn@tsinghua.edu.cn

Robert Fitzgerald
Department of Mathematics
Southern Illinois University
Carbondale, IL 62901-4408
U.S.A.
Email: rfitzg@siu.edu

Michael D. Fried
3548 Prestwick Rd.
Billings, MT 59101
U.S.A.
Email: mfried@math.uci.edu

Lei Fu
Chern Institute of Mathematics
Nankai University
Tianjin 300071
P. R. China
Email: leifu@nankai.edu.cn

Shuhong Gao
Department of Mathematical Sciences
Clemson University
Clemson, SC 29634-0975
U.S.A.
Email: sgao@clemson.edu

Moubariz Z. Garaev
Centro de Ciencias Matemáticas
Universidad Nacional Autónoma de México
Morelia 58089, Michoacán
México
Email: garaev@matmor.unam.mx

Arnaldo Garcia
Instituto Nacional de Matemática Pura
e Aplicada, IMPA
Estrada Dona Castorina 110
22460-320, Rio de Janeiro, RJ
Brazil
Email: garcia@impa.br

Joachim von zur Gathen
B-IT, Universität Bonn
Dahlmannstr. 2
53179 Bonn
Germany
Email: gathen@bit.uni-bonn.de

Mark Giesbrecht
Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario, N2L 3G1
Canada
Email: mwg@uwaterloo.ca

Guang Gong
Department of Electrical and Computer
Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1
Canada
Email: ggong@uwaterloo.ca

David Goss
Department of Mathematics
Ohio State University
231 West 18th Avenue
Columbus, OH 43210
U.S.A.
Email: goss@math.ohio-state.edu

Roderick Gow
School of Mathematical Sciences
University College Dublin
Belfield, Dublin 4
Ireland
Email: rod.gow@ucd.ie

Kishan Chand Gupta
Applied Statistics Unit
Indian Statistical Institute
203 B. T. Road
Kolkata 700108
India
Email: kishan@isical.ac.in

Dirk Hachenberger
Institut für Mathematik
Universität Augsburg
86135 Augsburg
Germany
Email: hachenberger@math.uni-augsburg.de

M. Anwarul Hasan
Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, ON, N2L 3G1
Canada
Email: ahasan@uwaterloo.ca

Tor Helleseth
Institutt for informatikk
Universitetet i Bergen
PB. 7803, N-5020 Bergen
Norway
Email: Tor.Helleseth@ii.uib.no

Franziska Hinkelmann
Mathematical Biosciences Institute
Ohio State University
1735 Neil Ave
Columbus, OH 43210
U.S.A.
Email: hinkelmann.1@mbi.osu.edu

James W.P. Hirschfeld
Department of Mathematics
University of Sussex
Brighton BN1 9QH
United Kingdom
Email: jwph@sussex.ac.uk

Xiang-dong Hou
Department of Mathematics and Statistics
University of South Florida
4202 E. Fowler Ave
Tampa, FL 33620
U.S.A.
Email: xhou@usf.edu

W. Cary Huffman
Department of Mathematics and Statistics
Loyola University Chicago
1032 W. Sheridan Road
Chicago, IL 60660
U.S.A.
Email: whuffma@luc.edu

Michael Jacobson, Jr.
Department of Computer Science
University of Calgary
Calgary, Alberta, T2N 1N4
Canada
Email: jacobs@ucalgary.ca

Jonathan Jedwab
Department of Mathematics
Simon Fraser University
Burnaby, British Columbia V5A 1S6
Canada
Email: jed@sfu.ca

Dieter Jungnickel
Mathematical Institute
University of Augsburg
D-86135 Augsburg
Germany
Email: jungnickel@math.uni-augsburg.de

Erich Kaltofen
Department of Mathematics
Campus Box 8205
North Carolina State University
Raleigh, NC 27695-8205
U.S.A.
Email: kaltofen@math.ncsu.edu

Alexander Kholosha
Department of Informatics
University of Bergen
P.O. Box 7800
N-5020 Bergen
Norway
Email: Alexander.Kholosha@uib.no

Melsik Kyuregyan
Institute for Informatics and Automation Problems
National Academy of Sciences of Armenia
1, P. Sevak str., Yerevan 0014
Armenia
Email: melsik@ipia.sci.am

Tanja Lange
Coding Theory and Cryptology, MF6.104 B
Department of Mathematics and Computer Science
Technische Universiteit Eindhoven
P.O. Box 513
5600 MB Eindhoven
Netherlands
Email: tanja@hyperelliptic.org

Reinhard Laubenbacher
Virginia Bioinformatics Institute
Blacksburg, VA 24061
U.S.A.
Email: reinhard@vbi.vt.edu

Grégoire Lecerf
Laboratoire d'informatique (LIX, UMR 7161 CNRS)
Campus de l'École polytechnique
Bátiment Alan Turing
91128 Palaiseau Cedex
France
Email: gregoire.lecerf@math.cnrs.fr

Hendrik Lenstra
Mathematisch Institut
Universiteit Leiden
Postbus 9512
2300 RA Leiden
The Netherlands
Email: hwl@math.leidenuniv.nl

Antonio Rojas-León
Departamento de Álgebra - Facultad de Matemáticas
Universidad de Sevilla
Apdo. de correos 1160
41080 Sevilla
Spain
Email: arojas@us.es

Qunying Liao
Institute of Mathematics and Software Science
Sichuan Normal University
Chengdu, Sichuan Province, 610066
P. R. China
Email: qunyingliao@sicnu.edu.cn

Rudolf Lidl
7 Hill Street
West Launceston
Tasmania 7250
Australia
Email: rudi@rlidl.com.au

Simon Litsyn
School of Electrical Engineering
Tel Aviv University
Ramat Aviv 69978
Israel
Email: litsyn@eng.tau.ac.il

Gary McGuire
School of Mathematical Sciences
University College Dublin
Dublin 4
Ireland
Email: gary.mcguire@ucd.ie

Wilfried Meidl
Faculty of Engineering and Natural Sciences
Sabanci University
Orhanli 34956, Tuzla-Istanbul
Turkey
Email: wmeidl@sabanciuniv.edu

Alfred Menezes
Department of Combinatorics & Optimization
University of Waterloo
Waterloo, Ontario N2L 3G1
Canada
Email: ajmeneze@uwaterloo.ca

Gary L. Mullen
Department of Mathematics
The Pennsylvania State University
University Park, PA 16802
U.S.A.
Email: mullen@math.psu.edu

Kumar Murty
Department of Mathematics
University of Toronto
40 St. George Street
Toronto, ON M5S 2E4
Canada
Email: murty@math.toronto.edu

M. Ram Murty
Department of Mathematics and Statistics
Queen's University
Kingston, Ontario K7L 3N6
Canada
Email: murty@mast.queensu.ca

Harald Niederreiter
Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences
Altenbergerstr. 69
A-4040 Linz
Austria
Email: ghnied@gmail.com

Andrew Odlyzko
School of Mathematics
University of Minnesota
Minneapolis, MN 55455
U.S.A.
Email: odlyzko@umn.edu

Alina Ostafe
Department of Computing
Faculty of Science
Macquarie University
North Ryde, NSW 2109
Australia
Email: alina.ostafe@mq.edu.au

Daniel Panario
School of Mathematics and Statistics
Carleton University
Ottawa ON K1S 5B6
Canada
Email: daniel@math.carleton.ca

Clément Pernet
INRIA/LIG MOAIS
51, avenue Jean Kuntzmann
F-38330 Montbonnot Saint-Martin
France
Email: clement.pernet@imag.fr

Alexander Pott
Otto-von-Guericke University Magdeburg
39106 Magdeburg
Germany
Email: alexander.pott@ovgu.de

Martin Roetteler
NEC Laboratories America, Inc.
4 Independence Way, Suite 200
Princeton, NJ 08540
U.S.A.
Email: mroetteler@nec-labs.com

Ivelisse Rubio
Department of Computer Science
University of Puerto Rico
Rio Piedras Campus
P.O. Box 70377
San Juan, PR 00936-8377
Email: iverubio@gmail.com

Renate Scheidler
Department of Mathematics and Statistics
University of Calgary
2500 University Drive NW
Calgary, Alberta, T2N 1N4
Canada
Email: rscheidl@ucalgary.ca

Kai-Uwe Schmidt
Faculty of Mathematics
Otto-von-Guericke University
Universitätsplatz 2
39106 Magdeburg
Germany
Email: kaiuwe.schmidt@ovgu.de

Igor Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109
Australia
Email: igor.shparlinski@mq.edu.au

Joseph H. Silverman
Mathematics Department, Box 1917
Brown University
Providence, RI 02912
U.S.A.
Email: jhs@math.brown.edu

Bart de Smit
Mathematisch Institut
Universiteit Leiden
Postbus 9512
2300 RA Leiden
The Netherlands
Email: desmit@math.leidenuniv.nl

Brett Stevens
School of Mathematics and Statistics
Carleton University
Ottawa ON K1S 5B6
Canada
Email: brett@math.carleton.ca

Henning Stichtenoth
Faculty of Engineering and Natural Sciences
Sabanci University
Orhanli 34956, Tuzla-Istanbul
Turkey
Email: henning@sabanciuniv.edu

Leo Storme
Department of Mathematics
Ghent University
Krijgslaan 281, Building S22
B-9000 Ghent, Belgium
Email: ls@cage.ugent.be

Oscar Takeshita
Email: oscar_takeshita@hotmail.com

Joseph A. Thas
Department of Mathematics
Ghent University
Krijgslaan 281 - S22
9000 Gent
Belgium
Email: jat@cage.ugent.be

Nicolas Thériault
Departamento de Matemática
Universidad del Bio-Bio
Avda. Collao 1202
Casilla 5-C, Concepcion, 4051381
Chile
Email: ntheriau@ubiobio.cl

David Thomson
School of Mathematics and Statistics
Carleton University
Ottawa ON K1S 5B6
Canada
Email: dthomson@math.carleton.ca

José Felipe Voloch
The University of Texas at Austin
Mathematics Dept, RLM 8.100
2515 Speedway Stop C1200
Austin, Texas 78712-1202
U.S.A.
Email: voloch@math.utexas.edu

Daqing Wan
Department of Mathematics
University of California
Irvine, CA 92697-3875
U.S.A.
Email: dwan@math.uci.edu

Zhe-Xian Wan
Academy of Mathematics and Systems Science
Chinese Academy of Sciences
No 55, Zhongguancun East Road
Zhongguancun, Beijing 100190
P. R. China
Email: wan@amss.ac.cn

Qiang Wang
School of Mathematics and Statistics
Carleton University
Ottawa ON K1S 5B6
Canada
Email: wang@math.carleton.ca

Arne Winterhof
Johann Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences
Altenbergerstr. 69
4040 Linz, Austria
Email: arne.winterhof@oeaw.ac.at

Joseph L. Yucas
68 Rock Springs Rd.
Makanda, IL 62958
U.S.A.
Email: joeyucas@yahoo.com

Michael E. Zieve
Department of Mathematics
University of Michigan
Ann Arbor, MI 48109-1043
U.S.A.
Email: zieve@umich.edu

This page intentionally left blank

I

Introduction

This page intentionally left blank

1

History of finite fields

1.1 Finite fields in the 18-th and 19-th centuries

Roderick Gow, *University College Dublin*

1.1.1 Introduction

While the theory of finite fields emerged as an independent discipline at the end of the 19-th century, aspects of the subject can be traced back at least to the middle of the 17-th century. It is our intention to present here a survey of highlights of finite field theory as they emerged in the 18-th and 19-th centuries, culminating in a description of Eliakim Hastings Moore's [2139], which began the study of abstract finite fields.

Leonard Eugene Dickson (1874-1954), in the first volume of his *History of the Theory of Numbers* [851] gives many references to works that can be interpreted as dealing with finite fields, although not always described explicitly as such. Chapters VII and VIII are especially relevant, and give remarkably complete listings of what had been achieved before 1918. Chapter VIII, entitled *Higher Congruences*, occasionally uses the language of finite fields, although the emphasis is largely number theoretic. Dickson had already written a textbook, entitled *Linear Groups with an Exposition of the Galois Field Theory* [850] which is probably the first work devoted exclusively to finite fields. This book remained without any serious rival until the emergence in the 1950s of more geometric, less computational, methods, such as those pioneered by Artin in his *Geometric Algebra* [135]. The first 71 pages of Dickson's work constitute a very full account of finite fields, and its exercises, partly based on the work of earlier researchers, are still a valuable source of problems and ideas.

Of course, finite fields are mentioned in general histories of algebra, such as that of van der Waerden [2848]. Furthermore, *Finite Fields* by Lidl and Niederreiter [1939] contains much historical information and a very extensive bibliography, especially of the older literature. Another brief but useful source of information is found in the historical notes scattered throughout Cox's *Galois Theory* [749].

The first use of the English expressions *field of order s* and *Galois-field of order* $s = q^n$ occurs in a paper of E. H. Moore (1862-1932), which he presented in 1893. Moore states that the term *field* was an equivalent to the German term *endlicher Körper*, used by Heinrich Weber (1842-1913). We observe that Richard Dedekind (1831-1916) had already introduced such a term as *Zahlenkörper*, which can be traced back to lectures he gave in 1858. The 1933 edition of the *Oxford English Dictionary* does not include a definition of the mathematical term *field*, although it does define *group* in its mathematical meaning, but more recent editions of the dictionary include the mathematical use of *field*, with an attribution to Moore.

The name Galois field is synonymous with finite field, and it signifies the importance to the subject of an innovatory paper by Évariste Galois (1811-1832), published in 1830 [1168], when the author was only 18. We will comment in greater detail on Galois's work later in this article, but we will briefly mention here that Galois lays the foundations of finite field theory by showing that for each prime p and positive integer n, there is a finite field of order p^n, and its multiplicative group of non-zero elements is cyclic of order $p^n - 1$.

Galois's arguments are rather sketchy, but there is no doubt that he understood the fundamental principles of the structure of a finite field, including the role of the automorphism given by raising elements to the p-th power. As has proved to be the case on a number of occasions, it seems that most of Galois's discoveries were already known to Gauss, in this case, in the late 1790s, but as Gauss never published an account of his work, Galois was unaware of Gauss's priority. (Gauss is credited with the discovery of non-Euclidean geometry before Bolyai and Lobachevsky, with the discovery of quaternions before Hamilton, and the discovery of the method of least squares before Legendre.) We will also give a sketch of Gauss's approach to finite fields, which he called the theory of *higher congruences*, as it is described in Volume 2 of his *Werke* [1259].

1.1.2 Early anticipations of finite fields

Our approach to the early history of finite fields will be largely chronological. An early occurrence of a theorem that may be interpreted in the language of finite fields is Fermat's Little Theorem, that $x^{p-1} - 1$ is divisible by p when p is a prime and x an integer not divisible by p. Dickson states that the special case when $x = 2$ was already known to the ancient Chinese around 500 BCE. As was usual with Fermat (1601-1665), he did not give a formal proof, but he communicated his conjecture that the theorem holds true, in a letter to Bernard Frénicle de Bessy (1605-1675), dated 18 October, 1640. Leonhard Euler (1707-1783) gave a complete proof of the theorem in 1736, but unpublished manuscripts of Gottfried Wilhelm Leibniz (1646-1716) show that he was in possession of a similar proof by 1680.

In the 18-th century, further theorems, expressed in terms of congruences modulo a prime, that we can see as precursors of basic facts in finite field theory were discovered by mathematicians such as Euler, Joseph-Louis Lagrange (1736-1813), and Adrien-Marie Legendre (1752-1833). However, the first complete account of that body of knowledge that relates to the finite field of prime order was presented by Carl Friedrich Gauss (1777-1855) in Sections I-IV of his *Disquisitiones Arithmeticae* [1258], which we describe in the next section.

1.1.3 Gauss's Disquisitiones Arithmeticae

Gauss's *Disquisitiones Arithmeticae* [1258] was an epoch making work in mathematics, introducing totally new ideas and demanding far higher standards of proof than had hitherto been required or expected. The book also serves as a commentary on the discoveries and shortcomings of his predecessors. For a very full account of the contents and influence of

Gauss's *magnum opus*, we refer to the book *The Shaping of Arithmetic* [1297].

Gauss introduces the concept of congruence in Article (Art.) 1, and designates congruence by means of the now familiar symbol $\equiv$. This is the first published use of this symbol, which seems to have entered into conventional use quite rapidly. It occurs for instance in C. Kramp's *Éléments d'arithmétique universelle* [1804] an elementary work much influenced by Gauss's masterpiece (the use of the exclamation mark in $n!$ makes its first appearance here). In Section 2, Gauss proves in Art. 14 that if p is a prime integer and a, b are integers not divisible by p, then p does not divide the product ab. This basic result is fundamental for the proof that the integers modulo p form a field. Gauss comments that the theorem was already in Euclid's *Elements*. Oddly enough, for a person as notoriously meticulous as Gauss, he mistakenly says that it is Proposition 32 of Book VII, when it is in fact Proposition 30. Concerning this result, Gauss wrote magisterially: *However we did not wish to omit it because many modern authors have employed vague computations in place of proof or have neglected the theorem entirely, and because by this very simple case we can more easily understand the nature of the method which will be used later for solving much more difficult problems.* He uses Art. 14 to prove Art. 16, a result often called the fundamental theorem of arithmetic: *a composite number can be resolved into prime factors in only one way.* This basic result is not in Euclid.

Gauss describes Euler's totient (or phi) function, which he denotes by the symbol ϕ (following Art. 38). (We recall that the totient function measures the number of totitives of a positive integer n, that is, the number of integers lying between 1 and n that are relatively prime to n.) This is again the first occurrence of a now familiar symbol in mathematics. Euler himself, although introducing the idea of the function in 1760, did not use such notation. Art. 43 is a proof that an integer polynomial of degree m cannot have more than m incongruent roots modulo a prime. This basic theorem on polynomial arithmetic was first published by Lagrange in 1768. Euler had shown that the congruence $x^n - 1 \equiv 0$ modulo a prime has at most n roots in 1774, and Gauss notes that Euler's method is easily generalized.

Section III, on residues of powers, contains Art. 49: *if p is a prime number that does not divide a, and a^t is the lowest power of a that is congruent to unity to the modulus p, the exponent t will either $= p - 1$ or be a factor of this number.* Gauss notes that this implies Fermat's Little Theorem, and he gives some of the history of this theorem that we described above. Art. 55 is the fundamental statement: *There always exist numbers with the property that no power less than the $p - 1$st is congruent to unity.* This of course amounts to saying that the multiplicative group of the integers modulo a prime p is cyclic of order $p - 1$. Again, it is interesting to observe the authority of Gauss's language as he describes earlier approaches to Art. 55: *This theorem furnishes an outstanding example of the need for circumspection in number theory so that we do not accept fallacies as certainties. ... No one has attempted the demonstration except Euler ... See especially his article 37 where he speaks at great length of the need for demonstration. But the demonstration which this shrewdest of men presents has two defects. ...* In Art. 57, Gauss adopts the nomenclature *primitive roots*, due originally to Euler, for the integers, or residues, described in Art. 55.

1.1.4 Gauss's Disquisitiones Generales de Congruentiis

Gauss had intended to include an eighth section of *Disquisitiones Arithmeticae*, and he even refers to this section at least twice in the published version. However, the section was omitted, possibly for reasons of saving space in an already long work. A manuscript of the missing section was found after Gauss's death, and an edited version, with notes by Dedekind, was published in volume 2 of Gauss's *Werke* [1259] in 1863, under the title *Disquisitiones Generales de Congruentiis*. A German translation followed in 1889.

Günther Frei, [1103], has given a lengthy description of the genesis and contents of the unpublished Section Eight, and we will make use of some of his analysis here, since it has considerable bearing on the early theory of finite fields. Gauss's work on finite fields can be traced back at least to 1796, as there are references to it in his *Mathematical Diary* [1257]. It is well known that Gauss was particularly fascinated by the law of quadratic reciprocity, and he gave several different proofs of this fundamental theorem, the first dating from 1796. The third and fourth of these proofs drew Gauss into the study of polynomials modulo a prime, and his surviving investigations enable us to discern much of the theory of finite extensions of a field of prime order.

In Frei's translation, Gauss wrote *But at the same time one sees that the solution of congruences constitutes only a part of a much higher investigation, namely the investigation of the decomposition of functions into factors.* Accordingly, Gauss developed a theory of factorization of polynomials whose coefficients are integers modulo a prime p, including the determination of greatest common divisors by Euclid's algorithm. He introduced the concept of a *prime* polynomial, corresponding to *irreducible* polynomial in modern terminology, and showed that arbitrary polynomials can be factored into products of prime polynomials.

Among the highlights of his discoveries, we may mention his proof that every irreducible polynomial modulo p, different from x, and of degree m, is a divisor of $x^{p^m-1}-1$. Furthermore, $x^{p^m-1}-1$ is the product of all monic irreducible polynomials of degree d dividing m, apart from x. From this fact, he obtained a formula for the number of irreducible monic polynomials of degree n with coefficients integers modulo p. Frei also notes that Gauss appreciated the importance of the *Frobenius automorphism*, and came close to discovering a form of Hensel's Lemma, significant in p-adic analysis.

The idea of using the imaginary roots of such irreducible polynomials to simplify some of his work had occurred to Gauss, and, in Frei's translation, Gauss wrote *Indeed, we could have shortened incomparably all our following investigations, had we wanted to introduce such imaginary quantities by taking the same liberty some more recent mathematicians have taken, but nevertheless, we have preferred to deduce everything from first principles.* It should be recalled that Gauss sometimes displayed a conservative approach to new concepts in mathematics, and his public aversion to using imaginary roots of congruences is akin to his disinclination to use complex numbers. Thus, for example, his thesis, published in 1799, states that every real polynomial is a product of real factors of degree one or two, rather than stating that every complex polynomial is a product of factors of degree 1.

1.1.5 Galois's Sur la théorie des nombres

We turn now to presenting a synopsis of Galois's 1830 paper [1168] *Sur la théorie des nombres* on finite fields since it is a landmark in the subject. In Frei's opinion, Galois establishes the additive and multiplicative structure of finite extensions of the field of prime order. It certainly seems that the spirit of Galois's paper is closer to the modern presentation of finite field theory than Gauss's version. It is worth noting that there are several misprints in the paper, which would have made it difficult to follow for the uninitiated, and Galois's attempts to illustrate the theory are hopelessly flawed.

Rather than translating the original French literally, we will instead try to convey some idea in modern terms of what Galois must have intended. For example, when Galois talks of a *function*, he means a polynomial in a single variable, with integer coefficients. (This convention was common among mathematicians before the twentieth century.) He notes that we usually look for integer roots of the polynomial modulo a prime p, say. We call these *real* roots of the polynomial congruence. He proceeds to generalize the notion of real roots, and begins by introducing the concept of an integer polynomial $F(x)$ being *irreducible* modulo p, meaning that it is impossible to find three integer polynomials $\phi(x)$, $\psi(x)$ and

$\chi(x)$ such that

$$F(x) + p\chi(x) = \phi(x)\psi(x).$$

(Galois does not use the term irreducible for this concept, but later in the paper speaks of an *irreducible congruence*.)

Such an irreducible polynomial $F(x)$ obviously has no integer roots modulo p, nor any *irrational roots* of degree less than that of $F(x)$ (Galois does not explain these terms). He states that we must regard the roots of the congruence $F(x) \equiv 0$ (notation he attributes to Gauss) as a type of imaginary symbols, and opines that such imaginary roots will prove to be as useful as $\sqrt{-1}$ is in conventional analysis. These imaginary roots were subsequently called *Galois imaginaries* by later writers.

Let i be a root of the congruence $F(x) \equiv 0$, where F has degree ν. (Galois does not justify why we may assume that $F(x) \equiv 0$ has roots, a point Serret attempted to rectify.) Galois then considers a general expression

$$a + a_1 i + a_2 i^2 + \cdots + a_{\nu-1} i^{\nu-1},$$

where a, a_1, $\ldots$, $a_{\nu-1}$ are integers modulo p. There are p^ν different values for these expressions.

Let α be an expression of the form above. If we raise α to the second, third, *etc*, powers, we obtain a sequence of expressions of the same form. Thus we must have $\alpha^n = 1$ for a certain positive integer n, which we choose to be as small as possible. We then have n different expressions

$$1, \alpha, \ldots, \alpha^{n-1}.$$

Galois shows that n divides $p^\nu - 1$, and thus $\alpha^{p^\nu - 1} = 1$. Galois next aims to prove that there is some α for which the corresponding n is $p^\nu - 1$. He makes an analogy at this stage with existence of primitive roots modulo p in the theory of numbers. We did not find that Galois provided a convincing argument for this key issue.

Galois then draws the remarkable conclusion that all the algebraic quantities that arise in this theory are roots of equations of the form $x^{p^\nu} = x$. Furthermore, if $F(x)$ is an integer polynomial of degree ν irreducible modulo p, there are integer polynomials $f(x)$ and $\phi(x)$ such that

$$f(x)F(x) = x^{p^\nu} - x + p\phi(x).$$

Galois also notes that if α is a root of the irreducible congruence $F(x) \equiv 0$, then the other roots are

$$\alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{\nu-1}}.$$

This is a consequence of the fact that

$$F(x)^{p^n} \equiv F(x^{p^n}).$$

We remark that this is an early indication of the role of the so-called Frobenius mapping as a generator of the associated Galois group. Galois later notes that all the roots of the congruence $x^{p^\nu} \equiv x$ depend only on the roots of a single irreducible polynomial of degree ν.

To illustrate all this theory, Galois attempts to find a primitive root of the congruence

$$x^{7^3} \equiv x \pmod 7.$$

He aims to do this by exhibiting elements having orders 9 and 19. In fact, he makes several noteworthy errors, which may have confused any readers of this exposition of the new theory. He begins by noting that $x^3 \equiv 2 \pmod 7$ is irreducible, and lets i be a root of the

congruence. He claims that $-1-i$ has order 19, but this is false, as it has order 9×19. He then claims that $\alpha = i + i^2$ is primitive, but this is again false, as it has order 114, not $342 = 7^3 - 1$. Finally, Galois claims that his α satisfies

$$\alpha^3 + 3\alpha + 1 = 0,$$

but this is again incorrect, as in truth it satisfies

$$\alpha^3 + \alpha + 1 = 0.$$

Indeed, the polynomial $x^3 + 3x + 1$ is not even irreducible modulo 7, as 4 is a root of it. As we mentioned earlier, the paper contains several misprints, possibly because the compositor found the notation difficult to handle, but Galois's errors are not just typographical (although they are of course ultimately trivial and in no way invalidate his theory).

Joseph-Alfred Serret gives a treatment of this problem of finding a primitive root in the second edition of *Cours d'algèbre supérieure* [2596], pp. 367-370, following Galois's methods. The required primitive element Galois might have had in mind was $\beta = i - i^2$, not $i + i^2$. This element β is a root of $x^3 - x + 2$, which is certainly an irreducible primitive polynomial. While $i + i^2$ may have replaced $i - i^2$ because of a typographical error, Galois nonetheless made further mistakes which are difficult to explain. Serret himself made no comment on this strange aspect of Galois's paper.

As justification for introducing this theory, Galois explains that it is required in the theory of permutations which arise in the study of primitive (rational) polynomials which are solvable by radicals. He alludes, in effect, to what is the affine group of the finite field of order p^ν, which must be the Galois group of such a polynomial when the action on the roots is doubly transitive. He excludes degrees 9 and 25, where he must have known that there exist exceptional doubly transitive solvable permutation groups. There is another one in degree 49, which he did not mention.

1.1.6 Serret's Cours d'algèbre supérieure

The early editions of Serret's textbook mentioned above provide us with a good opportunity to gauge the progress of the project to publicize Galois's research, considered very advanced at the time. In the first edition [2596], Serret writes that his (Serret's) work was a summary of lectures given at the Sorbonne, Paris, where he had been appointed to a chair in 1848. On p. 4, he notes that the difficult problem of when an equation can be solved algebraically had been resolved, at least in the case of irreducible equations of prime degree, by Évariste Gallois (*sic*), in a memoir of 1831. This memoir had been published in 1846 by Joseph Liouville in his *Journal*, and Liouville had wanted Serret to communicate part of Galois's findings. Lesson 23 of this first edition is devoted to the theory of congruence modulo a prime, but it includes nothing that was not already known at the time of Lagrange or Euler.

The second edition of Serret's work (1854) gives a fairly complete account of Galois's theory of finite fields, as presented in his 1830 paper. Serret devotes almost 30 pages (the whole of Lesson 25) to the material that Galois had covered in six pages, with a view to making a difficult part of the writings of this great mathematician more intelligible. Thus, for example, he proves a uniqueness theorem for factoring polynomials into irreducible factors, and also gives a lengthy discussion of why primitive elements exist. On the other hand, he does not attempt to give a rigorous explanation of why roots of irreducible congruences may be taken to exist. Lesson 25 seems to be the first exposure of finite fields at the textbook level.

Serret devotes 68 pages of the third edition of his textbook (1866) to the theory of finite fields. He considered his approach to be new, and based it on a memoir he had presented in

1865. In fact, it bears many similarities to Gauss's unpublished Section 8 (itself published for the first time in Latin in 1863), and to Dedekind's 1857 paper (for details, see later in this section). Serret was presumably unaware of this material, as he made no mention of it. We can recognize several classical theorems of finite field theory described clearly in Serret's Chapter 3 of Volume 2 of the third edition. Thus for example, if the integer g is not divisible by the prime p, the polynomial (later said to be of Artin-Schreier type)

$$x^p - x - g$$

is irreducible modulo p. Art. 372 presents six theorems summarizing Galois's findings of 1830, Art. 349 gives a formula for the number of monic irrreducible polynomials modulo a prime p, and Art. 350 gives upper and lower bounds for their number.

1.1.7 Contributions of Schönemann and Dedekind

Another early contribution to finite field theory is a paper by Theodor Schönemann, *Grundzüge einer allgemeinen Theorie der Höheren Congruenzen, deren Modul eine reele Primzahl ist* [2556] published in 1845. Schönemann is described as an *oberlehrer* (head teacher) at the Gymnasium in Brandenburg. He begins his paper with an apology, acknowledging that Gauss's unpublished Section 8 was to contain contributions to the theory of higher congruences, and that he (Schönemann) may have inadvertently rediscovered some of Gauss's results. Schönemann starts with a monic integer polynomial f of degree n which is irreducible modulo a prime p. He then takes a complex root α of f and considers in effect the quotient ring, $\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha]$, which is a finite field of order p^n. In this way, he avoids the question of whether imaginary roots of irreducible congruences may be taken to exist. This is described well in Cox [749], p. 296. One of Schönemann's main theorems is that if we allow α also to represent a root of f modulo p, then

$$f \equiv (x-\alpha)(x-\alpha^p)\cdots(x-\alpha^{p^{n-1}}) \pmod{p}.$$

He also obtained a formula for the number of monic irreducible polynomials of degree n modulo p. Schönemann's paper is long (56 pages) and not very clear. It is also written in a very formal style, each result being presented in the form of *Erklärung* and *Lehrsatz*, followed by *Beweis*, in imitation of the approach characteristic of Euclid's *Elements*. Nonetheless, Schönemann did innovatory work, which, even if anticipated by Gauss, was quoted reasonably frequently in the second half of the nineteenth century, for instance, by Kronecker.

In his paper *Abriss einer Theorie der Höheren Congruenzen in Bezug auf einen reellen Primzahl-Modulus* [793] written in late 1856, and published in 1857, Dedekind covered much of the same ground pioneered by Gauss in *Disquisitiones Generales de Congruentiis*. While we pointed out above that Dedekind was responsible for editing Gauss's manuscript for publication in 1863, Frei presents several strong reasons to suppose that, at the time he wrote, Dedekind was unacquainted with this key work, and did not see it until 1860. Frei suggests that Dedekind was more concerned to give a solid foundation to Kummer's theory of ideal numbers. In any case, Dedekind notes that there is a strong analogy between the theory of polynomials modulo a prime and elements of number theory. By way of illustrating this analogy, let p be an odd prime and let P and Q be different irreducible monic polynomials of degrees m and n, respectively. Then working modulo Q, P determines an element of the field of order p^n, and this element is either a square or a non-square. By analogy with the Legendre symbol, we set $(\frac{P}{Q})$ equal to 1 if P is a square modulo Q, and $(\frac{P}{Q})$ equal to -1 if it is a non-square. Working modulo P, we may likewise define $(\frac{Q}{P})$. Then, in complete

analogy with the law of quadratic reciprocity, we have

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{(\frac{p-1}{2})mn}.$$

In his proof, Dedekind uses a version of Gauss's Lemma, employed in one of Gauss's proofs of the quadratic reciprocity theorem.

1.1.8 Moore's characterization of abstract finite fields

Towards the end of the 19th century, finite fields began to assume a more prominent position in contemporary algebraic research, partly because of their importance in the construction of finite analogues of the classical linear groups. Camille Jordan, in his *Traité des substitutions* [1621] had investigated classical groups, such as the general linear group (also called the linear homogeneous group), over finite fields of prime order. E. H. Moore observed that certain of these constructions could be extended to arbitrary finite fields and he discovered the simple groups usually denoted by $\mathrm{PSL}_2(q^n)$. (He became aware by 1895 that these groups were already known to Émile Mathieu, who had come across them in 1860, [2021], pp. 38-42.) In any case, Moore was led to the investigation of abstract finite fields.

We quote from Moore's paper *A doubly infinite system of simple groups*, read on August 25, 1893, at the International Mathematical Congress held in Chicago [2139]. This paper gives the details of Moore's discoveries.

Suppose that we have a system of s distinct symbols or marks *(s being some positive integer) and suppose that these marks may be combined by the four fundamental operations of algebra–addition, subtraction, multiplication, and division–these operations being subject to the ordinary abstract* operational identities *of algebra*

$$\mu_i + \mu_j = \mu_j + \mu_i; \quad \mu_i\mu_j = \mu_j\mu_i; \quad (\mu_i + \mu_j)\mu_k = \mu_i\mu_k + \mu_j\mu_k; \ \textit{etc},$$

and that when the marks are so combined the results of these operations are in every case uniquely determined and belong to the system of marks. Such a system of marks we shall call a field of order *s, using the notation* $F[s]$. ...

We are led at once to seek [t]*o determine all such fields of order s,* $F[s]$.

Moore notes that Galois had defined a field of order q^n, for each prime q and each positive integer n. Moore denotes this field by $GF[q^n]$, presumably in honor of Galois. This $GF[q^n]$ is defined via an irreducible polynomial of degree n modulo q, and is unique, in the sense that such irreducible polynomials exist for all q and n, and the $GF[q^n]$ so constructed is independent of the particular irreducible polynomial chosen. Moore's main theorem is then stated as: *Every existent field* $F[s]$ *is the abstract form of a Galois field* $GF[q^n]$*;* $s = q^n$. Moore remarks: *This interesting result I have not seen stated before.*

Moore's proof occupies pages 212-220 of his paper, and he derives further properties of $GF[q^n]$ in the next few pages. We feel that Moore's paper marks the beginning of the abstract theory of finite fields. In 1896, Dickson was awarded the first doctorate in mathematics at the new University of Chicago, for a thesis written under Moore's direction, the subject matter being permutation polynomials over finite fields. Dickson's 1901 book gave a streamlined proof of Moore's uniqueness theorem on pp. 13-14.

1.1.9 Later developments

Following the work of his thesis, Dickson was to extend Jordan's analysis of classical groups to their counterparts over arbitrary finite fields, and his research was the subject of his monograph of 1901. Dickson even generalized ideas of Élie Cartan on continuous groups

and their Lie algebras, and published in 1901 (with later additions) details of his discovery of versions of the groups of type E_6 and G_2 over finite fields [842, 848, 843, 844]. It was not until later work of Chevalley in 1955 that further finite analogues of the exceptional continuous groups were constructed in a uniform way.

The theory of finite fields may be said to have acquired a more conceptual form in the twentieth century after Emil Artin (1898-1962) introduced the notion of a zeta function for a quadratic extension of the rational function field $\mathbf{F}_p(t)$, where p is a prime. Artin formulated a version of the Riemann hypothesis for these zeta functions, and verified the hypothesis for a number of curves in his dissertation, published in 1924. Helmut Hasse (1899-1979) subsequently proved the Riemann hypothesis for function fields of genus 1 in 1934, but the complete proof for arbitrary non-singular curves by André Weil (1906-1998) in 1948 employed sophisticated methods of algebraic geometry. The analogy between counting rational points on algebraic varieties over finite fields and the cohomology theories of complex varieties has been a powerful motivating force in the more recent theory of finite fields.

References Cited: [135, 749, 793, 842, 843, 844, 848, 850, 851, 1168, 1257, 1258, 1259, 1297, 1621, 1804, 1939, 2021, 2139, 2556, 2596, 2848]

This page intentionally left blank

2

Introduction to finite fields

2.1 Basic properties of finite fields

Gary L. Mullen, *The Pennsylvania State University*
Daniel Panario, *Carleton University*

Proofs for most of the results in this chapter can be found in Chapters 2 and 3 of [1939]; see also [1631, 1938, 2017, 2049, 2077, 2179, 2921]. We refer the reader to Section 2.1.8 for a comprehensive list of other finite field related books.

2.1.1 Basic definitions

2.1.1 **Definition** A *ring* $(R, +, \cdot)$ is a nonempty set R together with two operations, "+" and "$\cdot$" such that:

(1) $(R, +)$ is an abelian group;
(2) $\cdot$ is associative, that is for all $a, b, c \in R, a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
(3) left and right distributive laws hold: for all $a, b, c \in R$

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

2.1.2 **Definition** Let R be a ring.
(1) R is a *ring with identity* if the ring has a multiplicative identity;
(2) R is *commutative* if "$\cdot$" is commutative;
(3) R is an *integral domain* if it is commutative with identity and $a \cdot b = 0$ implies $a = 0$ or $b = 0$, for any $a, b \in R$;

(4) R is a *division ring* (also called a *skew field*) if the nonzero elements of R form a group under "$\cdot$";
(5) R is a *field* if it is a commutative division ring.

2.1.3 Definition The *order of a finite field* $\mathbb{F}$ is the number of distinct elements in $\mathbb{F}$.

2.1.4 Remark The following theorem is a famous result due to Wedderburn.

2.1.5 Theorem Every finite division ring is a field.

2.1.6 Definition If R is a ring and there exists a positive integer n such that $nr = 0$ for all $r \in R$, then the least such positive integer n is the *characteristic* of the ring, and R has *positive characteristic*. Otherwise, R has *characteristic zero*.

2.1.7 Theorem A ring $R \neq \{0\}$ of positive characteristic having an identity and no zero divisors must have prime characteristic.

2.1.8 Corollary A finite field has prime characteristic.

2.1.9 Proposition For a commutative ring R of characteristic p, we have

$$(a_1 + \cdots + a_s)^{p^n} = a_1^{p^n} + \cdots + a_s^{p^n}$$

for every $n \geq 1$ and $a_i \in R$.

2.1.2 Fundamental properties of finite fields

2.1.10 Lemma Suppose F is a finite field with a subfield K containing q elements. Then F is a vector space over K and $|F| = q^m$, where m is the dimension of F viewed as a vector space over K.

2.1.11 Definition A field containing no proper subfield is a *prime field*.

2.1.12 Theorem Let F be a finite field. The cardinality of F is p^n, where p is the characteristic of F and n is the dimension of F over its prime subfield.

2.1.13 Remark We denote by $\mathbb{F}_q$ a finite field with q elements. We note that by Remark 2.1.34 there is only one finite field (up to isomorphism) with q elements.

2.1.14 Remark Another common notation for a field of order q is $GF(q)$, where GF stands for Galois field. This name is used in honor of Évariste Galois (1811–1832), who in 1830 was the first person to seriously study properties of general finite fields (fields with a prime power but not necessarily a prime number of elements).

2.1.15 Remark The recent publication of *The Mathematical Writings of Evariste Galois* by Neumann [2223] will make Galois's own words available to readers.

2.1.16 Lemma If $\mathbb{F}_q$ is a finite field with q elements and $a \neq 0 \in \mathbb{F}_q$, then $a^{q-1} = 1$, and thus $a^q = a$, for all a in $\mathbb{F}_q$.

2.1.17 Remark An immediate consequence of the previous lemma is that the multiplicative inverse of any $a \neq 0$ in a field of order q is a^{q-2}, because $a^{q-2} \cdot a = a^{q-1}$.

2.1.18 Theorem The sum of all elements of a finite field is 0, except for the field $\mathbb{F}_2$.

2.1.19 **Definition** A polynomial f over $\mathbb{F}_q$ is an expression of the form $f(x) = \sum_{i=0}^{n} a_i x^i$, where n is a nonnegative integer, and $a_i \in \mathbb{F}_q$ for $i = 0, 1, \ldots, n$. A polynomial is *monic* if the coefficient of the highest power of x is 1. The ring formed by the polynomials over $\mathbb{F}_q$ with sum and product of polynomials is the *ring of polynomials over* $\mathbb{F}_q$ and is denoted by $\mathbb{F}_q[x]$.

2.1.20 **Definition** A polynomial $f \in \mathbb{F}_q[x]$ is an *irreducible polynomial* over $\mathbb{F}_q$ if f has positive degree and $f = gh$ with $g, h \in \mathbb{F}_q[x]$ implies that either g or h is a constant polynomial.

2.1.21 **Remark** Both $\mathbb{F}_q[x]$ and the ring of polynomials in $n \geq 1$ variables, $\mathbb{F}_q[x_1, \ldots, x_n]$, have unique factorization into irreducibles.

2.1.22 **Definition** The Möbius μ function is defined on the set of positive integers by

$$\mu(m) = \begin{cases} 1 & \text{if } m = 1, \\ (-1)^k & \text{if } m = m_1 m_2 \cdots m_k, \text{ where the } m_i \text{ are distinct primes,} \\ 0 & \text{otherwise, i.e., if } p^2 \text{ divides } m \text{ for some prime } p. \end{cases}$$

2.1.23 **Definition** The number of monic irreducible polynomials of degree n over $\mathbb{F}_q$ is denoted by $I_q(n)$.

2.1.24 **Theorem** For all $n \geq 1$ and any prime power q, we have

$$I_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

2.1.25 **Remark** We have that $I_q(n) > 0$ for all prime powers q and all integers $n > 1$:

$$I_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d} \geq \frac{1}{n} \left(q^n - q^{n-1} - q^{n-2} - \cdots - q \right) > 0.$$

2.1.26 **Remark** For a polynomial $f \in \mathbb{F}_q[x]$, we have $(f(x))^q = f(x^q)$. This property is of great use in finite field calculations.

2.1.27 **Lemma** If $\mathbb{F}_q$ is a finite field with q elements then in $\mathbb{F}_q[x]$ we have

$$x^q - x = \prod_{a \in \mathbb{F}_q} (x - a).$$

2.1.28 **Remark** The next theorem is crucial for fast polynomial irreducibility testing and factorization algorithms over finite fields; see Sections 11.3 and 11.4.

2.1.29 **Theorem** Let f be an irreducible polynomial of degree n over $\mathbb{F}_q$. Then $f(x) | (x^{q^r} - x)$ if and only if $n | r$.

2.1.30 **Definition** Let $f \in F[x]$ be of positive degree and E an extension of F. Then f *splits* in E if f can be written as a product of linear factors in $E[x]$, that is, there exist $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$ such that

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

where $a \in F$ is the leading coefficient of f and E is the smallest such field. The field E is a *splitting field* of f over F if f splits in E.

2.1.31 **Theorem** If F is a field, and f any polynomial of positive degree in $F[x]$, then there exists a splitting field of f over F. Any two splitting fields of f over F are isomorphic under an isomorphism which keeps the elements of F fixed and maps the roots of f into each other.

2.1.32 **Theorem** For every prime p and positive integer $n \geq 1$ there is a finite field with p^n elements. Any finite field with p^n elements is isomorphic to the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.

2.1.33 **Remark** The previous theorem shows that a finite field of a given order is unique up to field isomorphism because splitting fields are unique up to isomorphism. Thus we speak of "the" finite field of a particular order q.

2.1.34 **Remark** We note that when p is a prime the field $\mathbb{F}_p$ is the same as (isomorphic to) the ring $\mathbb{Z}_p$ of integers modulo p. The ring $\mathbb{Z}_p$ is also denoted by $\mathbb{Z}/p\mathbb{Z}$. When $n > 1$ the finite field $\mathbb{F}_{p^n}$ is not the same as the ring $\mathbb{Z}_{p^n}$ of integers modulo p^n. Indeed, $\mathbb{Z}_{p^n}$ is not a field if $n > 1$.

2.1.35 **Theorem** Let $\mathbb{F}_{p^n}$ be the finite field with p^n elements. Every subfield of $\mathbb{F}_{p^n}$ has p^m elements for some positive integer m dividing n. Conversely, for any positive integer m dividing n there is a unique subfield of $\mathbb{F}_{p^n}$ of order p^m.

2.1.36 **Remark** The subfields of $\mathbb{F}_{q^{36}}$ are illustrated in the following diagram:

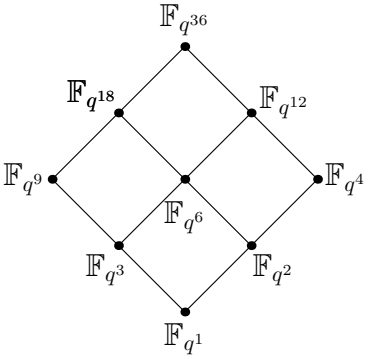


Figure 2.1.1 The subfields of $\mathbb{F}_{q^{36}}$.

2.1.37 **Theorem** The multiplicative group $\mathbb{F}_q^*$ of all nonzero elements of the finite field $\mathbb{F}_q$ is cyclic.

2.1.38 **Definition** An element $\alpha \in \mathbb{F}_q$ which multiplicatively generates the group $\mathbb{F}_q^*$ of all nonzero elements of the field $\mathbb{F}_q$ is a *primitive element*, sometimes also a *primitive root*.

2.1.39 **Remark** Let θ be a primitive element of a finite field $\mathbb{F}_q$. Then every nonzero element of $\mathbb{F}_q$ can be written as a power of θ. This representation makes multiplication of field elements

very easy to compute. However, in general, it may not be easy to find the power s of θ such that $\theta^t + \theta^r = \theta^s$; see Subsection 2.1.7.5. Conversely, as we will see later in our discussion of bases for finite fields, representations which make exponentiation easy to compute often have a more complex multiplicative structure.

2.1.40 **Definition** Let $\alpha \in \mathbb{F}_q^*$. The *order* of α is the smallest positive integer n such that $\alpha^n = 1$.

2.1.41 **Remark** We use the notation (a, b) or $\gcd(a, b)$ to represent the *greatest common divisor (gcd)* of a and b, where a and b belong to a Euclidean domain (usually integers or polynomials).

2.1.42 **Lemma** If g is a primitive element of $\mathbb{F}_q$ then g^t is a primitive element of $\mathbb{F}_q$ if and only if $(t, q-1) = 1$.

2.1.43 **Definition** The number of positive integers $e \leq n$ such that $(n, e) = 1$ is denoted by $\phi(n)$, and is the *Euler function*.

2.1.44 **Remark** The Euler function is multiplicative: if $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

2.1.45 **Remark** It follows from Lemma 2.1.42 that there are exactly $\phi(q-1)$ primitive elements in $\mathbb{F}_q$.

2.1.46 **Definition** A monic polynomial all of whose roots are primitive elements is a *primitive polynomial*.

2.1.47 **Remark** Primitive polynomials are treated in Chapter 4.

2.1.48 **Definition** The *reciprocal* f^* of a monic polynomial f of degree n is defined by $f^*(x) = x^n f(1/x)$. The polynomial f is *self-reciprocal* if $f^* = f$.

2.1.49 **Remark** The reciprocal polynomial of an irreducible polynomial f, $f(x) \neq x$, over $\mathbb{F}_q$ is again irreducible over $\mathbb{F}_q$. In addition, the *monic* reciprocal polynomial defined by $f(x)/f(0)$ of a primitive polynomial is also primitive.

2.1.50 **Remark** If f is a self-reciprocal irreducible polynomial of degree $n > 1$, in $\mathbb{F}_q[x]$, then n must be even.

2.1.51 **Definition** Let $f \in \mathbb{F}_q[x]$ be a nonzero polynomial. If $f(0) \neq 0$, the *order* of f is the least positive integer e such that $f | x^e - 1$. If $f(0) = 0$, let $f(x) = x^r g(x)$ for some integer $r \geq 1$ and $g \in \mathbb{F}_q[x]$ with $g(0) \neq 0$. In this case, the order of f is the order of g.

2.1.52 **Remark** We denote the order of f by $\mathrm{ord}(f)$. The order of a polynomial is also called the *period* or *exponent* of the polynomial.

2.1.53 **Theorem** Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial over $\mathbb{F}_q$ of degree n with $f(0) \neq 0$. Then $\mathrm{ord}(f)$ is equal to the order of any root of f in the multiplicative group of $\mathbb{F}_{q^n}^*$.

2.1.54 **Corollary** If $f \in \mathbb{F}_q[x]$ is an irreducible polynomial over $\mathbb{F}_q$ of degree n, then $\mathrm{ord}(f) | (q^n - 1)$.

2.1.55 **Theorem** Let $\mathbb{F}_q$ be a finite field of characteristic p, and let $f \in \mathbb{F}_q[x]$ be a polynomial of positive degree with $f(0) \neq 0$. Let $f = a f_1^{b_1} \cdots f_k^{b_k}$ be the canonical factorization of f into irreducibles in $\mathbb{F}_q[x]$, where $a \in \mathbb{F}_q, b_1, \ldots, b_k \in \mathbb{N}$, and $f_1, \ldots, f_k$ are distinct monic irreducible polynomials in $\mathbb{F}_q[x]$. Then $\mathrm{ord}(f) = ep^t$, where e is the least common multiple of $\mathrm{ord}(f_1), \ldots, \mathrm{ord}(f_k)$ and t is the smallest integer with $p^t \geq \max(b_1, \ldots, b_k)$.

2.1.3 Extension fields

2.1.56 **Definition** Let K be a subfield of F and let M be a subset of F. Then $K(M)$ denotes the intersection of all subfields of F containing K and M as subsets. This field is K *adjoin* M. When M is finite, say $M = \{\alpha_1, \ldots, \alpha_k\}$, we write $K(\alpha_1, \ldots, \alpha_k)$ for $K(M)$.

2.1.57 **Definition** Let $K \subseteq F$, $\alpha \in F$, and $f(\alpha) = 0$ where f is a monic polynomial in $K[x]$. Then f is the *minimal polynomial* of α if α is not a root of any nonzero polynomial in $K[x]$ of lower degree.

2.1.58 **Proposition** The minimal polynomial of any extension field element is irreducible over the base field. This result provides a method by which one can obtain irreducible polynomials.

2.1.59 **Definition** A field F is a *finite extension* of K if $K \subseteq F$ and F is a finite dimensional vector space over K. In this case we refer to the dimension m of F over K as the *degree* of the extension, and we write $[F : K] = m$.

2.1.60 **Theorem** Let F be a finite extension of K and let E be a finite extension of F. Then E is a finite extension of K. Moreover, we have $[E : K] = [E : F][F : K]$.

2.1.61 **Definition** Let $K \subseteq F$ and let $\alpha \in F$. Then α is *algebraic* over K if there is a nonzero polynomial $f \in K[x]$ such that $f(\alpha) = 0$ in $F[x]$. An extension field is *algebraic* if every element of the extension field is algebraic.

2.1.62 **Theorem** Every finite extension of a field is algebraic.

2.1.63 **Theorem** Let K be a subfield of F with $\alpha \in F$ algebraic of degree n over K and let g be the minimal polynomial of α over K. Then:

1. The field $K(\alpha)$ is isomorphic to the factor ring $K[x]/(g)$.
2. The dimension of $K(\alpha)$ over K is n.
3. The set $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for $K(\alpha)$ over K.
4. Every element of $K(\alpha)$ is algebraic over K with degree dividing n.

2.1.64 **Remark** An extension obtained by adjoining a single element is a *simple* extension. The next theorem gives an important property of finite fields which is not shared by infinite fields (there are finite extensions of infinite fields which are not simple).

2.1.65 **Theorem** Let $\mathbb{F}_q$ be a finite field and let $\mathbb{F}_r$ be a finite extension of $\mathbb{F}_q$. Then $\mathbb{F}_r$ is a simple algebraic extension of $\mathbb{F}_q$, and for any primitive element α of $\mathbb{F}_r$ the relation $\mathbb{F}_r = \mathbb{F}_q(\alpha)$ holds.

2.1.66 **Corollary** For any prime power q and any integer $n \geq 1$ there is an irreducible polynomial of degree n over $\mathbb{F}_q$.

2.1.67 **Example** Consider $q = 2^{100}$. We can identify the elements of $\mathbb{F}_q$ with polynomials of the form $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{99}\alpha^{99}$, where $0 \leq a_i < 2$ for each i and where α is a root of an irreducible polynomial of degree 100 over the field $\mathbb{F}_2$. Corollary 2.1.66 shows that such an irreducible polynomial always exists. Using Theorem 2.1.24 we have that there are exactly

$$\frac{1}{100}\left(2^{100} - 2^{50} - 2^{20} + 2^{10}\right)$$

irreducible polynomials of degree 100 over $\mathbb{F}_2$.

2.1.68 Remark Corollary 2.1.66 can also be derived using the formula for the number of irreducible polynomials in Theorem 2.1.24.

2.1.69 Example Consider the polynomial $f(x) = x^2+x+1$ over the field $\mathbb{F}_2$. Since f does not have a root in $\mathbb{F}_2$, f is irreducible over $\mathbb{F}_2$. Let α be a root of f so that $\alpha^2+\alpha+1=0$, that is, $\alpha^2 = -(\alpha+1) = \alpha+1$. The field $\mathbb{F}_4 = \mathbb{F}_{2^2}$ can be represented as the set $\{a\alpha+b\colon a,b\in\mathbb{F}_2\}$. We give the addition and multiplication tables for the field $\mathbb{F}_{2^2}$. We note that α is a primitive element in the field $\mathbb{F}_4$, so $\alpha^1=\alpha, \alpha^2=\alpha+1$ and $\alpha^3=1$.

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\times$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

2.1.70 Example Consider the field $\mathbb{F}_9$, which is a vector space of dimension 2 over $\mathbb{F}_3$. Consider $f(x) = x^2+x+2$ in $\mathbb{F}_3[x]$. This polynomial has no roots in $\mathbb{F}_3$ so it is irreducible over $\mathbb{F}_3$. Let α be a root of f, so $\alpha^2+\alpha+2=0$. Hence $\alpha^2 = -\alpha-2 = 2\alpha+1$. The field $\mathbb{F}_{3^2}$ is isomorphic to the set $\{a\alpha+b \mid a,b\in\mathbb{F}_3\}$ with its natural operations. We can compute the addition and multiplication tables by hand. For example, $2\alpha(\alpha+2) = 2\alpha^2+4\alpha = 2(2\alpha+1)+\alpha = 2\alpha+2$. The following addition and multiplication tables are obtained. We can use the multiplication table to check that the multiplicative order of α in $\mathbb{F}_9$ is 8, and thus α is a primitive element of $\mathbb{F}_9$.

$+$	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
1	1	2	0	$\alpha+1$	$\alpha+2$	α	$2\alpha+1$	$2\alpha+2$	2α
2	2	0	1	$\alpha+2$	α	$\alpha+1$	$2\alpha+2$	2α	$2\alpha+1$
α	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$	0	1	2
$\alpha+1$	$\alpha+1$	$\alpha+2$	α	$2\alpha+1$	$2\alpha+2$	2α	1	2	0
$\alpha+2$	$\alpha+2$	α	$\alpha+1$	$2\alpha+2$	2α	$2\alpha+1$	2	0	1
2α	2α	$2\alpha+1$	$2\alpha+2$	0	1	2	α	$\alpha+1$	$\alpha+2$
$2\alpha+1$	$2\alpha+1$	$2\alpha+2$	2α	1	2	0	$\alpha+1$	$\alpha+2$	α
$2\alpha+2$	$2\alpha+2$	2α	$2\alpha+1$	2	0	1	$\alpha+2$	α	$\alpha+1$

$\times$	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
2	0	2	1	2α	$2\alpha+2$	$2\alpha+1$	α	$\alpha+2$	$\alpha+1$
α	0	α	2α	$2\alpha+1$	1	$\alpha+1$	$\alpha+2$	$2\alpha+2$	2
$\alpha+1$	0	$\alpha+1$	$2\alpha+2$	1	$\alpha+2$	2α	2	α	$2\alpha+1$
$\alpha+2$	0	$\alpha+2$	$2\alpha+1$	$\alpha+1$	2α	2	$2\alpha+2$	1	α
2α	0	2α	α	$\alpha+2$	2	$2\alpha+2$	$2\alpha+1$	$\alpha+1$	1
$2\alpha+1$	0	$2\alpha+1$	$\alpha+2$	$2\alpha+2$	α	1	$\alpha+1$	2	2α
$2\alpha+2$	0	$2\alpha+2$	$\alpha+1$	2	$2\alpha+1$	α	1	2α	$\alpha+2$

2.1.71 Example Let $f(x) = x^2+1 \in \mathbb{F}_3[x]$. It is straightforward to check that f is irreducible over the field $\mathbb{F}_3$. Let α be a root of f. We compute $\alpha^2 = -1$ and $\alpha^4 = 1$. Hence no root of f can have order 8, that is, no root of f can be a primitive element. Nevertheless, the splitting field of f over $\mathbb{F}_3$ is $\mathbb{F}_9$. It can be seen that $\alpha+1$ has order 8 and is thus a primitive element for $\mathbb{F}_9$ over $\mathbb{F}_3$.

2.1.72 Remark Tables of irreducible and primitive polynomials can be found in Section 2.2. In that section is a discussion of some computer algebra packages for implementing finite field arithmetic.

2.1.73 Theorem If f is an irreducible polynomial of degree n over $\mathbb{F}_q$ then f has a root α in $\mathbb{F}_{q^n}$. Moreover all of the roots of f are simple and are given by $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$.

2.1.74 Definition Let $\alpha \in \mathbb{F}_{q^n}$. Then $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$ are the *conjugates* of α over $\mathbb{F}_q$.

2.1.75 Lemma Let $\alpha \in \mathbb{F}_{q^n}$ and let the minimal polynomial of α over $\mathbb{F}_q$ have degree d. Consider the set $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$ of conjugates of α. The elements of this set are distinct if $n = d$; otherwise each distinct conjugate is repeated n/d times.

2.1.76 Theorem The distinct automorphisms of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ are given by the functions $\sigma_0, \sigma_1, \ldots, \sigma_{n-1}$ where $\sigma_j : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ and is defined by $\sigma_j(\alpha) = \alpha^{q^j}$ for any $\alpha \in \mathbb{F}_{q^n}$.

2.1.77 Remark The set of automorphisms of $\mathbb{F}_q$ forms a group with the operation of functional composition. This group is called the *Galois group of* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$. It is a cyclic group with generator $\sigma_1 : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ that maps $\alpha \in \mathbb{F}_{q^n}$ to α^q, and is called the *Frobenius automorphism*. The conjugates of α are thus the elements to which α is sent by iterated applications of the Frobenius automorphism.

2.1.78 Remark The subfields of $\mathbb{F}_{q^n}$ are exactly the fields of the form $\mathbb{F}_{q^m}$ where $m|n$. The subgroups of the Galois group of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ are exactly the groups generated by σ_1^m where $m|n$. Moreover, $\sigma_1^m(\alpha) = \alpha$ if and only if $\alpha \in \mathbb{F}_{q^m}$. Thus there is a one-to-one correspondence between the subfields of $\mathbb{F}_{q^n}$ and the subgroups of its Galois group.

2.1.79 Remark In general, if F is an extension of a field K then the set of automorphisms of F that leave K fixed pointwise is the Galois group of F over K. The field of *Galois theory* is the study of Galois groups. Thus, if K is finite and F is a finite extension of K then the Galois group is cyclic. When K is infinite, the Galois group need not be cyclic, even if F is a finite extension of K.

2.1.4 Trace and norm functions

2.1.80 Definition Let $K = \mathbb{F}_q$ and $F = \mathbb{F}_{q^n}$. For $\alpha \in F$, we define the *trace* of α over K as $\mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}$. Equivalently, $\mathrm{Tr}_{F/K}(\alpha)$ is the sum of the conjugates of α. If K is the prime subfield of F then the trace function is the *absolute trace*.

2.1.81 Example Let $K = \mathbb{F}_2$ and $F = \mathbb{F}_{2^4}$. Then $\mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^2 + \alpha^4 + \alpha^8$. For $K = \mathbb{F}_4$ and $F = \mathbb{F}_{16}$ we have $\mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^4$.

2.1.82 Remark Since $\big(\mathrm{Tr}_{F/K}(\alpha)\big)^q = \mathrm{Tr}_{F/K}(\alpha)$ the trace of an element always lies in the base field K.

2.1.83 Theorem Let $K = \mathbb{F}_q$ and $F = \mathbb{F}_{q^n}$. The trace function has the following properties:

1. for any $\alpha \in F$, $\mathrm{Tr}_{F/K}(\alpha) \in K$;
2. $\mathrm{Tr}_{F/K}(\alpha + \beta) = \mathrm{Tr}_{F/K}(\alpha) + \mathrm{Tr}_{F/K}(\beta)$ for $\alpha, \beta \in F$;
3. $\mathrm{Tr}_{F/K}(c\alpha) = c\mathrm{Tr}_{F/K}(\alpha)$ for $\alpha \in F$ and $c \in K$;
4. the trace function is a K-linear map from F onto K;

5. $\mathrm{Tr}_{F/K}(\alpha) = n\alpha$ for $\alpha \in K$;
6. $\mathrm{Tr}_{F/K}(\alpha^q) = \mathrm{Tr}_{F/K}(\alpha)$ for $\alpha \in F$;
7. for any $\alpha \in K$, we have $|\{\beta \in F \mid \mathrm{Tr}_{F/K}(\beta) = \alpha\}| = q^{n-1}$;
8. Suppose that $K \subseteq F \subseteq E$ are finite fields; then for any $\alpha \in E$

$$\mathrm{Tr}_{E/K}(\alpha) = \mathrm{Tr}_{F/K}(\mathrm{Tr}_{E/F}(\alpha)).$$

2.1.84 Theorem For $\beta \in F$ let L_β be the map $\alpha \mapsto \mathrm{Tr}_{F/K}(\beta\alpha)$. Then $L_\beta \neq L_\gamma$ if $\beta \neq \gamma$. Moreover the K-linear transformations from F to K are exactly the maps of the form L_β as β varies over the elements of the field F.

2.1.85 Remark The result in Theorem 2.1.84 provides a method to generate all of the linear transformations from the extension field F to the subfield K.

2.1.86 Definition Let $K = \mathbb{F}_q$ and $F = \mathbb{F}_{q^n}$. The *norm* over K of an element $\alpha \in F$ is defined by

$$\mathrm{Norm}_{F/K}(\alpha) = \alpha\alpha^q \cdots \alpha^{q^{n-1}} = \prod_{i=0}^{n-1} \alpha^{q^i} = \alpha^{(q^n-1)/(q-1)}.$$

2.1.87 Remark The norm of an element α is thus calculated by taking the product of all of the conjugates of α, just as the trace of α is obtained by taking the sum of all of the conjugates of α.

2.1.88 Theorem Let $K = \mathbb{F}_q$ and $F = \mathbb{F}_{q^n}$. The norm function has the following properties:

1. $\mathrm{Norm}_{F/K}(\alpha) \in K$;
2. $\mathrm{Norm}_{F/K}(\alpha\beta) = \mathrm{Norm}_{F/K}(\alpha)\,\mathrm{Norm}_{F/K}(\beta)$ for $\alpha, \beta \in F$;
3. the norm maps F onto K and F^* onto K^*;
4. $\mathrm{Norm}_{F/K}(\alpha) = \alpha^n$ if $\alpha \in K$;
5. $\mathrm{Norm}_{F/K}(\alpha^q) = \mathrm{Norm}_{F/K}(\alpha)$;
6. if $K \subseteq F \subseteq E$ are finite fields then

$$\mathrm{Norm}_{E/K}(\alpha) = \mathrm{Norm}_{F/K}(\mathrm{Norm}_{E/F}(\alpha))\,.$$

2.1.5 Bases

2.1.89 Remark Every finite field F is a vector space over each of its subfields, and thus has a vector space basis over each of its subfields. There are several different kinds of bases for finite fields. Each kind of basis facilitates certain computations. When doing computations in finite fields, there are some important operations like addition, multiplication, q-th powering and finding inverses. With some bases computing inverses and q-th powers are easy, while multiplication could be more involved. With other bases, one can calculate multiplications quickly at the cost of more complicated inverse computations or exponentiations.

2.1.90 Remark The vector space of all $n \times r$ matrices over a field $\mathbb{F}_q$ is of dimension nr over $\mathbb{F}_q$. Taking into account the order of the elements, the total number of distinct bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is given by

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}),$$

which is also equal to the number of elements in the general linear group $GL_n(\mathbb{F}_q)$, the ring of nonsingular $n \times n$ matrices over $\mathbb{F}_q$.

2.1.91 Remark Consider $\mathbb{F}_{q^n}$ as a vector space over $\mathbb{F}_q$ of dimension n. We know there are many bases for this vector space. Given $B = \{\alpha_1, \ldots, \alpha_n\} \subseteq \mathbb{F}_{q^n}$, how can we tell if B is a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$? We begin with a test which determines whether a set of elements of $\mathbb{F}_{q^n}$ is independent over $\mathbb{F}_q$. If this result is applied to a set containing n elements, it can thus be used to determine whether these elements form a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. We require the following notation.

2.1.92 Definition Let $K = \mathbb{F}_q$ and $F = \mathbb{F}_{q^n}$. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a set of n elements of $\mathbb{F}$ viewed as a vector space over the subfield K. We define the *discriminant* $\Delta_{\mathbb{F}/K}(\alpha_1, \ldots, \alpha_n)$ with the following rule:

$$\Delta_{\mathbb{F}/K}(\alpha_1, \ldots, \alpha_n) = \begin{vmatrix} \mathrm{Tr}_{F/K}(\alpha_1\alpha_1) & \cdots & \mathrm{Tr}_{F/K}(\alpha_1\alpha_n) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}_{F/K}(\alpha_n\alpha_1) & \cdots & \mathrm{Tr}_{F/K}(\alpha_n\alpha_n) \end{vmatrix}.$$

2.1.93 Theorem If $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^n}$, then the set $\{\alpha_1, \ldots, \alpha_n\}$ is a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $\Delta_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_1, \ldots, \alpha_n)$ is nonzero.

2.1.94 Remark The following result provides an alternative method to determine if a given set of elements forms a basis. We note that the calculations for this method must be done in the extension field, not in the base field. Working in the extension field may have a significant computational cost. For example, if the base field is $\mathbb{F}_2$ and the extension field is $\mathbb{F}_{2^{1000}}$ then computations in the base field are much faster than computations in the extension field.

2.1.95 Corollary The set $\{\alpha_1, \ldots, \alpha_n\}$ is a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if

$$\begin{vmatrix} \alpha_1 & \cdots & \alpha_n \\ \alpha_1^q & \cdots & \alpha_n^q \\ \vdots & \ddots & \vdots \\ \alpha_1^{q^{n-1}} & \cdots & \alpha_n^{q^{n-1}} \end{vmatrix} \neq 0.$$

2.1.96 Definition Let α be a root of an irreducible polynomial of degree n over $\mathbb{F}_q$. The set $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a *polynomial basis* of the field $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

2.1.97 Remark When we use a polynomial basis for $\mathbb{F}_{q^n}$ we can regard field elements, which in reality are polynomials in α of degree at most $n-1$, as vectors. We can then easily add vectors in the usual way by adding the corresponding coefficients. Field multiplication is more complicated since we must gather terms with like powers of the basis elements when we simplify a product.

2.1.98 Definition If $\alpha \in \mathbb{F}_{q^n}$ and $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, then the basis is a *normal basis* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and α is a *normal element.*

2.1.99 Remark If $\beta = a_0\alpha + a_1\alpha^q + \cdots + a_{n-1}\alpha^{q^{n-1}}$ so that β is represented by the vector $(a_0, \ldots, a_{n-1})$, then α^q is simply represented by the shifted vector $(a_{n-1}, a_0, \ldots, a_{n-2})$. Thus if we have a normal basis, it is extremely easy to raise a field element to the power q. Addition is of course also still easy to compute using a normal basis. We note that multiplication of field elements is quite complicated using a normal basis. In Section 5.2 we

give important properties of normal bases including their existence for any finite extension field of $\mathbb{F}_q$.

2.1.100 **Definition** Two ordered bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_n\}$ are *complementary* (or *dual*) if $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_i \beta_j) = \delta_{ij}$, where $\delta_{ij} = 0$ if $j \neq i$ and $\delta_{ij} = 1$ if $i = j$. An ordered basis is *self-dual* if it is dual with itself.

2.1.101 **Definition** A *primitive normal basis* for an extension field $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is a basis of the form $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}\}$, where α is a primitive element for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

2.1.102 **Remark** Further kinds of bases for finite fields and their properties are discussed in detail in Chapter 5. For example, we show that each basis of $\mathbb{F}_{q^n}$ has a unique dual basis. We give fundamental properties of normal bases and primitive normal bases in Section 5.2. We give there, among other results, the fundamental theorem that for any prime power q and any integer $n \geq 2$ there exists a primitive normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

2.1.6 Linearized polynomials

2.1.103 **Definition** Let $L(x) = \sum_{i=0}^{n-1} \alpha_i x^{q^i}$, where $\alpha_i \in \mathbb{F}_{q^n}$. A polynomial of this form is a *linearized polynomial* over $\mathbb{F}_{q^n}$ (also a *q-polynomial* because the exponents are all powers of q).

2.1.104 **Remark** These polynomials form an important class of polynomials over finite fields because they are $\mathbb{F}_q$-linear functions from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^n}$.

2.1.105 **Theorem** Let $L(x)$ be a linearized polynomial. Then for all $\alpha, \beta \in \mathbb{F}_{q^n}$ and all $c \in \mathbb{F}_q$, we have

1. $L(\alpha + \beta) = L(\alpha) + L(\beta)$,
2. $L(c\alpha) = cL(\alpha)$.

2.1.106 **Theorem** Let L be a nonzero linearized polynomial over $\mathbb{F}_{q^n}$ and assume that the roots of L lie in the field $\mathbb{F}_{q^s}$, an extension field of $\mathbb{F}_{q^n}$. Then each root of L has the same multiplicity, which is either 1, or a positive power of q.

2.1.107 **Remark** The Frobenius automorphism $x \mapsto x^q$ is one such example, and the trace function $\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{q^i}$ provides another important example of a linearized polynomial over $\mathbb{F}_q$.

2.1.108 **Definition** Let L be a linearized polynomial over $\mathbb{F}_{q^n}$. A polynomial of the form $A(x) = L(x) - \alpha$, for $\alpha \in \mathbb{F}_{q^n}$, is an *affine polynomial* over $\mathbb{F}_{q^n}$.

2.1.109 **Theorem** Let A be a nonzero affine polynomial over $\mathbb{F}_{q^n}$ and assume that the roots of A lie in the field $\mathbb{F}_{q^s}$, an extension field of $\mathbb{F}_{q^n}$. Then each root of A has the same multiplicity, which is either 1, or a positive power of q.

2.1.7 Miscellaneous results

2.1.110 **Remark** We collect here some concepts and results needed in later sections of the handbook.

2.1.7.1 The finite field polynomial Φ function

2.1.111 **Definition** For $f \in \mathbb{F}_q[x]$, $\Phi_q(f)$ denotes the number of polynomials over $\mathbb{F}_q$ which are of smaller degree than the degree of f and which are relatively prime to f. This is also the number of units in the ring $\mathbb{F}_q[x]/(f(x))$.

2.1.112 **Remark** Similarly to the corresponding properties for the Euler function from elementary number theory, we have the following result (see Lemma 3.69 of [1939] and Definition 2.1.43).

2.1.113 **Lemma** The function Φ_q has the following properties:

1. $\Phi_q(f) = 1$ if the degree of f is 0;
2. $\Phi_q(fg) = \Phi_q(f)\Phi_q(g)$ if f and g are relatively prime;
3. if f has degree $n \geq 1$ then

$$\Phi_q(f) = q^n(1 - q^{-n_1}) \cdots (1 - q^{-n_r}),$$

where $n_1, \ldots, n_r$ are the degrees of the distinct monic irreducible polynomials appearing in the unique factorization of f in $\mathbb{F}_q[x]$.

2.1.114 **Remark** One important consequence of Lemma 2.1.113 is that if f is irreducible of degree n over $\mathbb{F}_q$, then $\Phi_q(f^e) = q^{ne} - q^{n(e-1)}$ for any positive integer e.

2.1.7.2 Cyclotomic polynomials

2.1.115 **Remark** The following is a synopsis of properties of roots of unity and cyclotomic polynomials, which can be found in [1939, Chapters 2 and 3].

2.1.116 **Remark** Let n be a positive integer. The polynomial $x^n - 1$ has many special properties over any field. For example, $x^n - 1$ is the minimal polynomial of the Frobenius automorphism which generates the Galois group of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, which is useful when studying normal bases over finite fields, see Section 5.2. Many of the basic properties of cyclotomic polynomials (and their roots) hold over arbitrary fields, however in this section we restrict to the finite field case.

2.1.117 **Definition** The roots $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_{q^n}$ of the polynomial $x^n - 1 \in \mathbb{F}_q[x]$ are the *n-th roots of unity* over $\mathbb{F}_q$.

2.1.118 **Remark** The roots of any degree n polynomial over $\mathbb{F}_q$ must be in $\mathbb{F}_{q^n}$. Thus, the n-th roots of unity of $\mathbb{F}_q$ are all contained in $\mathbb{F}_{q^n}$.

2.1.119 **Theorem** Let n be a positive integer and let $\mathbb{F}_q$ be a finite field of characteristic p. If p does not divide n, the roots of unity form a cyclic group of order n with respect to multiplication in $\mathbb{F}_q^*$. Otherwise, let $n = mp^e$, where $e > 0$ and $\gcd(m, p) = 1$. Then $x^n - 1 = (x^m - 1)^{p^e}$ and the n-th roots of unity are the m-th roots of unity with multiplicity p^e.

2.1.120 **Definition** Let $\mathbb{F}_q$ be a finite field of characteristic p which does not divide n. Denote the cyclic group of n-th roots of unity as U_n. Suppose that U_n is generated by $\alpha \in \mathbb{F}_{q^n}$, that is $U_n = \langle \alpha \rangle$. Then α is a *primitive n-th root of unity* over $\mathbb{F}_q$.

2.1.121 **Definition** Let $\mathbb{F}_q$ have characteristic p, not dividing n, and let ζ be a primitive n-th root of unity over $\mathbb{F}_q$. Then the polynomial

$$Q_n(x) = \prod_{s=1 \, \gcd(s,n)=1}^{n} (x - \zeta^s)$$

is the *n-th cyclotomic polynomial over $\mathbb{F}_q$*.

2.1.122 **Remark** The n-th cyclotomic polynomial does not depend on the choice of primitive root of unity chosen, since ζ^s, $\gcd(s, n) = 1$, runs over all primitive n-th roots of unity.

2.1.123 **Theorem** Let $\mathbb{F}_q$ be a finite field with characteristic p which does not divide n. Then

1. $\deg(Q_n) = \phi(n)$;
2. $x^n - 1 = \prod_{d|n} Q_d(x)$;
3. the coefficients of $Q_n(x)$ lay within $\mathbb{F}_p$.

2.1.124 **Proposition** Let r be a prime and let k be a positive integer. Then

$$Q_{r^k}(x) = 1 + x^{r^{k-1}} + x^{2r^{k-1}} + \cdots + x^{(r-1)r^{k-1}}.$$

2.1.125 **Theorem** Suppose $\gcd(n, q) = 1$, then Q_n factors into $\phi(n)/d$ distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree d, where d is the order of q modulo n. Furthermore, $\mathbb{F}_{q^d}$ is the splitting field of any such factor.

2.1.126 **Corollary** The cyclotomic polynomial Q_n is irreducible over $\mathbb{F}_q$ if and only if $n = 4, r^k, 2r^k$, $k \geq 0$, where r is an odd prime and q is a primitive root modulo n.

2.1.127 **Proposition** Let p be a prime and let m and k be positive integers. The following properties of cyclotomic polynomials hold over any field for which they are defined:

1. $Q_{mp}(x) = Q_m(x^p)/Q_m(x)$, if p does not divide m;
2. $Q_{mp}(x) = Q_m(x^p)$, if p divides m;
3. $Q_{mp^k}(x) = Q_{mp}(x^{p^{k-1}})$;
4. $Q_{2n}(x) = Q_n(-x)$ if $n \geq 3$ and n is odd;
5. $Q_n(0) = 1$ if $n \geq 2$;
6. $Q_n(x^{-1})x^{\phi(n)} = Q_n(x)$ if $n \geq 2$;
7. $$Q_n(1) = \begin{cases} 0 & \text{if } n = 1, \\ p & \text{if } n = p^e, \\ 1 & \text{if } n \text{ has at least two distinct prime factors;} \end{cases}$$
8. $$Q_n(-1) = \begin{cases} -2 & \text{if } n = 1, \\ 0 & \text{if } n = 2, \\ p & \text{if } n = 2p^e, \\ 1 & \text{otherwise.} \end{cases}$$

2.1.128 **Theorem** Let n be a positive integer not divisible by the characteristic of $\mathbb{F}_q$. An explicit factorization of the Q_n over $\mathbb{F}_q$ is given by

$$Q_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)},$$

where μ is the Möbius function, see Definition 2.1.22.

2.1.129 Proposition Suppose $\gcd(n, q) = 1$, then Q_n is irreducible over $\mathbb{F}_q$ if and only if the multiplicative order of q modulo n is $\phi(n)$.

2.1.130 Theorem The product of all monic irreducible polynomials of degree n over $\mathbb{F}_q$, denoted $I(q, n; x)$, is given by

$$I(q, n; x) = \prod_m Q_m(x),$$

where the product is taken over all positive divisors m of $q^n - 1$ such that n is the multiplicative order of q modulo m.

2.1.7.3 Lagrange interpolation

2.1.131 Theorem If $f\colon \mathbb{F}_q \to \mathbb{F}_q$, there is a unique polynomial P_f with coefficients in $\mathbb{F}_q$ and of degree at most $q - 1$ so that P_f represents the function f, that is, $P_f(b) = f(b)$ for all $b \in \mathbb{F}_q$. In particular,

$$P_f(x) = \sum_{a \in \mathbb{F}_q} f(a)[1 - (x - a)^{q-1}].$$

2.1.132 Remark The property that every function over a finite commutative ring with identity can be represented by a polynomial with coefficients in that ring characterizes finite fields. In particular, if a finite commutative ring R with unity has the property that every function from the ring to itself can be represented by a polynomial with coefficients in the ring, then R is a finite field, and conversely.

2.1.133 Remark The Lagrange Interpolation Formula can also be stated in the following form: for $n \geq 0$, let $a_0, \ldots, a_n$ be $n + 1$ distinct elements of $\mathbb{F}_q$, and let $b_0, \ldots, b_n$ be $n + 1$ arbitrary elements of $\mathbb{F}_q$. Then, there exists exactly one polynomial $f \in \mathbb{F}_q[x]$ of degree less than or equal to n such that $f(a_i) = b_i$, $i = 0, \ldots, n$. This polynomial is given by

$$f(x) = \sum_{i=0}^{n} b_i \prod_{k=0, k \neq i}^{n} \frac{x - a_k}{a_i - a_k}.$$

2.1.134 Theorem Let $f\colon \mathbb{F}_q^n \to \mathbb{F}_q$. The polynomial $P_f(x_1, \ldots, x_n)$ represents f, that is, $P_f(b_1, \ldots, b_n) = f(b_1, \ldots, b_n)$ for all $(b_1, \ldots, b_n) \in \mathbb{F}_q^n$, where

$$P_f(x_1, \ldots, x_n) = \sum_{(a_1, \ldots, a_n) \in \mathbb{F}_q^n} f(a_1, \ldots, a_n)[1 - (x_1 - a_1)^{q-1}] \cdots [1 - (x_n - a_n)^{q-1}].$$

2.1.7.4 Discriminants

2.1.135 Definition Let f be a polynomial of degree n in $\mathbb{F}_q[x]$ with leading coefficient a, and with roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ in its splitting field, counted with multiplicity. The *discriminant* of f is given by

$$D(f) = a^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

2.1.136 Example The discriminant of $ax^2 + bx + c = a(x - \alpha_1)(x - \alpha_2)$ is

$$\begin{aligned} D(ax^2 + bx + c) &= a^2(\alpha_1 - \alpha_2)^2 = a^2\left((\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2\right) \\ &= a^2\left(b^2a^{-2} - 4ca^{-1}\right) = b^2 - 4ac. \end{aligned}$$

The discriminant of $ax^3 + bx^2 + cx + d$ is

$$D(ax^3 + bx^2 + cx + d) = b^2c^2 - 4b^3d - 4ac^3 - 27a^2d^2 + 18abcd.$$

2.1.137 Remark The discriminant of f is a polynomial in the coefficients of f. It is also a symmetric function in the roots of f and thus lies in $\mathbb{F}_q$. Clearly, f has a multiple root if and only if $D(f) = 0$.

2.1.138 Proposition An alternative formula for the discriminant of a polynomial f is

$$D(f) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f'(\alpha_i),$$

where f' denotes the derivative of the polynomial f.

2.1.7.5 Jacobi logarithms

2.1.139 Definition If the elements of $\mathbb{F}_q^*$ are represented as powers of a fixed primitive element $b \in \mathbb{F}_q$, then addition in $\mathbb{F}_q$ can be facilitated by using *Jacobi logarithms* (sometimes also called *Zech logarithms*) $L(n)$ defined by the equation $1 + b^n = b^{L(n)}$, where the case $b^n = -1$ is excluded.

2.1.140 Remark One can show that $b^m + b^n = b^{m+L(n-m)}$ whenever this is defined. Tables of Jacobi logarithms for fields of characteristic 2 and order at most 64 can be found on Table B of [1939]. Jacobi logarithms were first studied by Jacobi [1584].

2.1.7.6 Field-like structures

2.1.141 Remark In this subsection we briefly describe several algebraic systems that have many but perhaps not all of the properties of a field. We are indebted to John Sheekey (Università di Padova) for this section.

2.1.142 Definition A *left (resp. right) prequasifield* is a set Q together with two operations, "+" and "$\cdot$" such that:

(1) (Q, +) is an abelian group;

(2) for all $a, b, c \in Q$ there exist unique $x, y, z \in Q$ such that

$$a \cdot x = b \quad \text{and} \quad y \cdot a = b \quad \text{and} \quad a \cdot z = b \cdot z + c;$$

(3) left (resp. right) distributive laws hold: for all $a, b, c \in Q$

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad (resp.(b + c) \cdot a = b \cdot a + c \cdot a).$$

2.1.143 Definition Let Q be a left prequasifield.

(1) A left prequasifield is a *left quasifield* if it has a multiplicative identity.

(2) A left prequasifield is a *presemifield* if it is also a right prequasifield.

(3) A presemifield is a *semifield* if it has a multiplicative identity.

(4) A semifield is *commutative* if "$\cdot$" is commutative.

(5) A left quasifield is a *left nearfield* if "$\cdot$" is associative.

2.1.144 Remark All left prequasifields have prime power order. Left prequasifields coordinatize translation planes. The smallest left prequasifield which is not a field has order 9. The smallest semifield which is not a field has order 16. For more on the above structures see [807] or [1560].

2.1.145 Remark The multiplicative structure of a left prequasifield is a *quasigroup*. The multiplicative structure of a semifield is a *loop*. The multiplicative structure of a nearfield is a *group*.

2.1.146 Definition Let Q be a set together with two operations, "+" and "$\cdot$", containing additive identity 0 and multiplicative identity 1, such that:

(1) $(Q/\{0\}, \cdot)$ is a group;

(2) left and right distributive laws hold: for all $a, b, c \in Q$

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and } (b + c) \cdot a = b \cdot a + c \cdot a;$$

(3) there exists a unique element 0 such that for all $a \in Q$

$$a + 0 = 0 + a = a.$$

(4A) Q is a *neofield* if in addition to (1), (2) and (3) it satisfies for all $a, b \in Q$ there exist unique $x, y \in Q$ such that

$$a + x = b \quad \text{and} \quad y + a = b.$$

(4B) Q is a *division semiring* if in addition to (1), (2) and (3) above it also satisfies $+$ is associative and commutative.

2.1.147 Remark The additive structure of a neofield is a *loop*. The additive structure of a division semiring is a *commutative monoid*.

2.1.148 Remark For more properties of semirings see [1291]. Note that a division semiring in which multiplication is commutative is sometimes also referred to as a semifield, but this definition does not coincide with the previously defined structures.

2.1.149 Remark For more properties of neofields see [2343].

2.1.7.7 Galois rings

2.1.150 Remark We briefly describe Galois rings. We are indebted to Horacio Tapia-Recillas (Universidad Autónoma Metropolitana, Unidad Iztapalapa, México) for this subsection.

2.1.151 Remark Galois rings represent a natural (Galois) extension of the (local) modular ring of integers $\mathbb{Z}/p^m\mathbb{Z}$ where p is a prime and m a positive integer. Krull [1808] recognized their existence and later, Janusz [1593] and Raghavendran [2436] independently obtained additional properties of these rings. More details on Galois rings can be found in [283, 1409, 2045, 2921].

2.1.152 Definition Let $\mathbb{Z}/p^m\mathbb{Z}$ be the ring of integers modulo p^m, p a prime and $m > 1$ an integer. A monic irreducible (primitive) polynomial $f \in (\mathbb{Z}/p^m\mathbb{Z})[x]$ of degree n is a *monic basic irreducible* (*primitive*) if its reduction modulo p is *irreducible* (*primitive*) in $(\mathbb{Z}/p\mathbb{Z})[x]$.

2.1.153 Remark Monic basic irreducible (primitive) polynomials in $(\mathbb{Z}/p^m\mathbb{Z})[x]$ can be determined by means of Hensel's Lifting Lemma from monic irreducible (primitive) polynomials in $(\mathbb{Z}/p\mathbb{Z})[x]$.

2.1.154 Definition Let $f \in (\mathbb{Z}/p^m\mathbb{Z})[x]$ be a monic basic irreducible polynomial of degree n. Then the Galois ring determined by f is

$$GR(p^m, n) = (\mathbb{Z}/p^m\mathbb{Z})[x]/\langle f(x)\rangle,$$

where $\langle f(x)\rangle$ is the principal ideal of $(\mathbb{Z}/p^m\mathbb{Z})[x]$ generated by $f(x)$.

2.1.155 Remark With the above notation, an equivalent definition of a Galois ring is the following.

2.1.156 Definition Let $\mathbb{Z}$ be the ring of (rational) integers and let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree n such that its reduction modulo $p\mathbb{Z}$ is irreducible, then

$$GR(p^m, n) = \mathbb{Z}[x]/\langle p^m, f\rangle.$$

2.1.157 Remark The Galois ring $GR(p^m, n)$ can also be defined by means of the p-adic numbers in the following way.

2.1.158 Definition Let p be a prime, $\mathbb{Q}_p$ be the field of p-adic (rational) numbers and $\mathbb{Z}_p$ be the ring of p-adic integers (for details see [2588]). Let n be a positive integer and let ω be a $(p^n - 1)$ root of unity. Then $\mathbb{Q}_p(\omega)$ is an unramified Galois extension of degree n of $\mathbb{Q}_p$. Let $\mathbb{Z}_p[\omega]$ be the ring of elements of $\mathbb{Q}_p(\omega)$ integral over $\mathbb{Z}_p$. Let $p\mathbb{Z}_p[\omega]$ be the (unique) maximal ideal of $\mathbb{Z}_p[\omega]$ generated by p. Then the quotient $\mathbb{Z}_p[\omega]/p\mathbb{Z}_p[\omega]$ is a field isomorphic to the Galois field $\mathbb{F}_{p^n}$.

2.1.159 Definition With the notation as above let m be a positive integer and let $p^m\mathbb{Z}_p[\omega]$ be the principal ideal of $\mathbb{Z}_p[\omega]$ generated by p^m. Then the Galois ring $GR(p^m, n)$ is defined as:

$$GR(p^m, n) = \mathbb{Z}_p[\omega]/p^m\mathbb{Z}_p[\omega].$$

2.1.160 Remark This ring contains as a subring the ring of integers modulo p^m, $\mathbb{Z}/p^m\mathbb{Z}$, and can be thought of as an extension of $\mathbb{Z}/p^m\mathbb{Z}$ by adjoining a $(p^n - 1)$ root of unity ω:

$$GR(p^m, n) = (\mathbb{Z}/p^m\mathbb{Z})\,[\omega].$$

2.1.161 Theorem With the notation as above, the basic properties of the Galois ring $GR(p^m, n)$ are the following [283, 1409, 2045, 2921]:

1. $GR(p^m, n)$ contains $\mathbb{Z}/p^m\mathbb{Z}$ as a subring, it has characteristic p^m and cardinality p^{mn}. The integer m is the *nilpotency* index of the Galois ring.
2. The ring $GR(p^m, n)$ is local with maximal ideal $\mathcal{M} = \langle p\rangle = pGR(p^m, n)$ generated by p, and a principal ideal ring where any ideal is of the form $\langle p^i\rangle$ for $i = 0, 1, 2, \ldots, m$. Furthermore, it is a finite chain ring:

$$GR(p^m, n) = \langle p^0\rangle \supset \langle p\rangle \supset \cdots \supset \langle p^{m-1}\rangle \supset \langle p^m\rangle = \{0\}.$$

The ideal $\langle p^i\rangle$ has cardinality $p^{n(m-i)}$ for $i = 0, 1, \ldots, m$.

3. Each non-zero element of the Galois ring $GR(p^m, n)$ can be written as up^k, where u is a unit and $0 \leq k \leq m-1$. In this representation the integer k is unique and the unit u is unique modulo the ideal $\langle p^{m-k} \rangle$.
4. The canonical homomorphism $\phi : GR(p^m, n) \longrightarrow GR(p^m, n)/\mathcal{M}$, between the Galois ring and its residue field $GR(p^m, n)/\mathcal{M}$ is such that $\phi(\xi) = \overline{\xi}$ is a root of $\phi(f(x))$. The residue field is isomorphic to the Galois field $GF(p^n) = \mathbb{F}_{p^n}$ with p^n elements. Furthermore, $GF(p^n)^* = \langle \overline{\xi} \rangle$.
5. The Galois ring is a $(\mathbb{Z}/p^m\mathbb{Z})$-module:

$$GR(p^m, n) = (\mathbb{Z}/p^m\mathbb{Z})[\xi] = (\mathbb{Z}/p^m\mathbb{Z}) + \xi(\mathbb{Z}/p^m\mathbb{Z}) + \cdots + \xi^{n-1}(\mathbb{Z}/p^m\mathbb{Z}).$$

6. The group of units $\mathcal{U}$ of the Galois ring $GR(p^m, n)$ has the following structure:

$$\mathcal{U} = C \times G,$$

where C is a cyclic group of order $p^n - 1$ generated by ξ and G is an abelian group of order $p^{(m-1)n}$. Furthermore,

   (a) if p is odd, or if $p = 2$ and $m \leq 2$ then G is a direct product of n cyclic groups, each of order p^{m-1};

   (b) if $p = 2$ and $m \geq 3$ the group G is the direct product of a cyclic group of order 2, a cyclic group of order 2^{m-2} and $n-1$ cyclic groups each of order 2^{m-1}.

7. There is a subset $\mathcal{T}$ of $GR(p^m, n)$, the *Teichmüller* set of representatives of the Galois ring, such that any element $\beta \in GR(p^m, n)$ has a unique p-adic (multiplicative) representation:

$$\beta = \rho_0(\beta) + \rho_1(\beta)p + \cdots + \rho_{m-1}(\beta)p^{m-1},$$

where $\rho_i(\beta) \in \mathcal{T}$ for $0 \leq i \leq m-1$. The elements of the maximal ideal of the Galois ring correspond to $\rho_0(\beta) = 0$. There is a bijection, induced by the canonical homomorphism ϕ, between $\mathcal{T}$ and the residue field of the Galois ring $GR(p^m, n)$.
8. The Teichmüller set of representatives of the Galois ring can be taken as

$$\mathcal{T} = \{0, 1, \xi, \xi^2, \ldots, \xi^{q-2}\} = \{0\} \cup C,$$

where $q = p^n$.
9. Given a prime p and an integer $n > 1$, for each divisor r of n there is a unique Galois ring $GR(p^m, r)$, and any subring of the Galois ring $GR(p^m, n)$ is of this form.
10. For each positive integer t, there is a natural injective ring homomorphism $GR(p^m, n) \longrightarrow GR(p^m, nt)$.
11. There is a natural surjective ring homomorphism $GR(p^m, n) \longrightarrow GR(p^{m-1}, n)$ with kernel $\langle p^{m-1} \rangle$.
12. The group of automorphisms of the Galois ring $GR(p^m, n)$ is a cyclic group of order n.
13. The Galois ring $GR(p^m, n)$ is quasi-Frobenius.

2.1.162 Example $GR(p, n) = GF(p, n) = \mathbb{F}_{p^n}, \quad GR(p^m, 1) = (\mathbb{Z}/p^m\mathbb{Z})$.

2.1.163 Example [2045] The polynomial $f(x) = x^3 + x + 1 \in (\mathbb{Z}/2^2\mathbb{Z})[x]$ is monic basic irreducible over $(\mathbb{Z}/2^2\mathbb{Z})$. Then $GR(2^2, 3) = (\mathbb{Z}/2^2\mathbb{Z})[x]/\langle f(x) \rangle$.

2.1.164 Example [1409] The polynomial $g(x) = x^3 + 2x^2 + x - 1 \in (\mathbb{Z}/2^2\mathbb{Z})[x]$ is also monic basic irreducible over $(\mathbb{Z}/2^2\mathbb{Z})$. Then $GR(2^2, 3) = (\mathbb{Z}/2^2\mathbb{Z})[x]/\langle g(x)\rangle$.

2.1.165 Example [283] The polynomial $g(x) = x^3 - 2x^2 - x - 1 \in (\mathbb{Z}/2^3\mathbb{Z})[x]$ is monic basic irreducible over $(\mathbb{Z}/2^3\mathbb{Z})$. Then $GR(2^3, 3) = (\mathbb{Z}/2^3\mathbb{Z})[x]/\langle g(x)\rangle$.

2.1.8 Finite field related books

2.1.166 Remark We give a list of finite field related books, divided into categories and listed without duplication even though a number of these books could be listed in two or more categories.

2.1.8.1 Textbooks

2.1.167 Remark We begin by listing a number of books that could be used as textbooks. Reference [1939] by Lidl and Niederreiter is, by far, the most comprehensive. Other textbooks include Jungnickel [1631], Lidl and Niederreiter [1938], Masuda and Panario [2017], McEliece [2049], Menezes et al. [2077], Mullen and Mummert [2179], Small [2681], and Wan [2921, 2923].

2.1.8.2 Finite field theory

2.1.168 Remark We list a number of books dealing with various theoretical topics related to finite fields: [240, 398, 557, 850, 961, 1121, 1122, 1333, 1389, 1511, 1631, 1701, 1756, 1773, 1843, 1845, 1922, 1936, 1938, 1939, 2017, 2049, 2054, 2077, 2107, 2548, 2637, 2641, 2667, 2670, 2672, 2681, 2711, 2714, 2793, 2920, 2921, 2923, 2949, 2950].

2.1.8.3 Applications

2.1.169 Remark The use of finite fields in algebraic coding theory has been the focus for numerous books: [231, 270, 304, 311, 1558, 1943, 1945, 1991, 2252, 2281, 2404, 2405, 2819, 2820, 2849].

2.1.170 Remark Theoretical and applied aspects of cryptography have been treated in: [245, 312, 313, 661, 759, 762, 922, 1105, 1303, 1413, 1521, 1563, 1694, 1774, 2076, 2080, 2644, 2720].

2.1.171 Remark There have been several books on the applications of finite fields in combinatorics, especially in combinatorial design theory and finite geometries: [131, 141, 211, 260, 261, 262, 453, 484, 706, 785, 807, 819, 1509, 1510, 1515, 1560, 1875, 2445, 2719, 2781, 2851].

2.1.8.4 Algorithms

2.1.172 Remark Several books contain results on algorithmic and computational finite field topics. These include [761, 1227, 2632].

2.1.8.5 Conference proceedings

2.1.173 Remark The *Finite Fields and Applications Conferences (Fq n series)* have been held every two years (except 2005) since 1991. The proceedings from these conferences are: [663, 1636, 1870, 2052, 2181, 2182, 2184, 2185, 2187, 2197]. Other conference proceedings volumes include: [533, 535, 596, 869, 1057, 1228, 1306, 1316, 1436, 1478, 1480, 1928].

References Cited: [131, 136, 141, 211, 231, 240, 245, 260, 261, 262, 270, 304, 311, 312, 313, 398, 453, 484, 533, 535, 557, 596, 661, 663, 706, 759, 761, 762, 785, 797, 807, 819, 850,

869, 922, 961, 1057, 1105, 1121, 1122, 1227, 1228, 1291, 1303, 1306, 1316, 1333, 1389, 1413, 1436, 1478, 1480, 1509, 1510, 1511, 1515, 1521, 1558, 1560, 1563, 1570, 1584, 1631, 1636, 1694, 1701, 1756, 1773, 1774, 1843, 1845, 1848, 1875, 1922, 1928, 1936, 1938, 1939, 1943, 1945, 1991, 2017, 2049, 2052, 2054, 2076, 2077, 2080, 2107, 2144, 2179, 2181, 2182, 2184, 2185, 2187, 2197, 2223, 2252, 2280, 2281, 2343, 2404, 2405, 2445, 2548, 2632, 2637, 2641, 2644, 2667, 2670, 2672, 2681, 2711, 2714, 2719, 2720, 2781, 2793, 2819, 2820, 2849, 2851, 2920, 2921, 2923, 2949, 2950]

2.2 Tables

David Thomson, *Carleton University*

2.2.1 Remark Unless otherwise stated, all of the data given in this section was created by the author and, when possible, was verified with known results. Basic algorithms (for example, brute force) were preferred due to their reliability and ease of verification. Unless stated, all simulations were done in C/C++ using the NTL version 5.5.2 library [2633] for modular computations. NTL was compiled using the GMP version 4.3.2 library [2797] for multi-precision arithmetic. Extended and machine-readable versions of the tables found in this section can be found on the book's website [2180].

2.2.2 Remark Since most computer algebra packages can readily handle basic finite field computations, our aim is not to repeat tables whose purpose is to improve hand-calculations. For reference, we briefly recall the list of tables found in [1939].

Tables A and B are aids to perform fast arithmetic by hand over small finite fields. Table A is a list of all elements over small finite fields and their discrete logarithms with respect to a primitive element. Table B provides a list of *Jacobi's logarithms* $L(\cdot)$ for $\mathbb{F}_{2^n}$, $2 \leq n \leq 6$. These logarithms allow the computation of field elements by the relationship $\zeta^\alpha + \zeta^\beta = \zeta^{\alpha+L(\beta-\alpha)}$.

Table C provides a list of all monic irreducible polynomials of degree n over small prime fields. Particularly, these tables cover $p = 2$ and $n \leq 11$, $p = 3$ and $n \leq 7$, $p = 5$ and $n \leq 5$, $p = 7$ and $n \leq 4$.

Tables D, E, and F deal with primitive polynomials. Table D lists one primitive polynomial over $\mathbb{F}_2$ for degrees $n \leq 100$. Table E lists all quadratic primitive polynomials for $11 \leq p \leq 31$ and Table F lists one primitive polynomial of degree n over $\mathbb{F}_p$ for all $n \geq 2$ with $p < 50$ and $p^n < 10^9$.

2.2.1 Low-weight irreducible and primitive polynomials

2.2.3 Remark Low-weight irreducible polynomials are highly desired due to their efficiency in hardware and software implementations of finite fields. Irreducible polynomials of degree at least 2 over $\mathbb{F}_2$ must have an odd number of terms. The use of irreducible trinomials (having 3 terms) and, in their absence, irreducible pentanomials (having 5 terms) are useful; see, for example, [1413, Chapter 2]. For cryptographic use, the irreducible trinomial or pentanomial of lowest lexicographical order (for a fixed n, prefer the trinomial x^n+x^k+1 over $x^n+x^{k_1}+1$ when $k < k_1$, the analogue for pentanomials is obvious) is often preferred for transparency reasons. However, the irreducible with the optimal performance for a given implementation is not necessarily the lowest lex-order, see [2573] and Section 11.1. A list of the lowest-weight

lowest-lex-order irreducible over $\mathbb{F}_2$ is given in [2582] for degree $n \leq 10000$. Table 2.2.1 gives the lowest-weight, lowest-lex-order irreducible polynomial for $n \leq 1025$. The output of the table follows the format n, k (for trinomials $x^n + x^k + 1$) or n, k_1, k_2, k_3 (for pentanomials $x^n + x^{k_1} + x^{k_2} + x^{k_3} + 1$). We have extended these tables to larger n and to larger q for small values of n. Furthermore, the computer algebra package Magma [712] contains similar tables, due to Steel (2004-2007), for the following values of q and n:

q	$n \leq$	q	$n \leq$	q	$n \leq$	q	$n \leq$
2	120,000	3	50,000	4, 5, 7	2000	$9 \leq q \leq 127$	1000 (or more).

Sections 3.4 and 4.3 give more information on weights of irreducible and primitive polynomials.

2,1	3,1	4,1	5,2	6,1	7,1	8,4,3,1	9,1
10,3	11,2	12,3	13,4,3,1	14,5	15,1	16,5,3,1	17,3
18,3	19,5,2,1	20,3	21,2	22,1	23,5	24,4,3,1	25,3
26,4,3,1	27,5,2,1	28,1	29,2	30,1	31,3	32,7,3,2	33,10
34,7	35,2	36,9	37,6,4,1	38,6,5,1	39,4	40,5,4,3	41,3
42,7	43,6,4,3	44,5	45,4,3,1	46,1	47,5	48,5,3,2	49,9
50,4,3,2	51,6,3,1	52,3	53,6,2,1	54,9	55,7	56,7,4,2	57,4
58,19	59,7,4,2	60,1	61,5,2,1	62,29	63,1	64,4,3,1	65,18
66,3	67,5,2,1	68,9	69,6,5,2	70,5,3,1	71,6	72,10,9,3	73,25
74,35	75,6,3,1	76,21	77,6,5,2	78,6,5,3	79,9	80,9,4,2	81,4
82,8,3,1	83,7,4,2	84,5	85,8,2,1	86,21	87,13	88,7,6,2	89,38
90,27	91,8,5,1	92,21	93,2	94,21	95,11	96,10,9,6	97,6
98,11	99,6,3,1	100,15	101,7,6,1	102,29	103,9	104,4,3,1	105,4
106,15	107,9,7,4	108,17	109,5,4,2	110,33	111,10	112,5,4,3	113,9
114,5,3,2	115,8,7,5	116,4,2,1	117,5,2,1	118,33	119,8	120,4,3,1	121,18
122,6,2,1	123,2	124,19	125,7,6,5	126,21	127,1	128,7,2,1	129,5
130,3	131,8,3,2	132,17	133,9,8,2	134,57	135,11	136,5,3,2	137,21
138,8,7,1	139,8,5,3	140,15	141,10,4,1	142,21	143,5,3,2	144,7,4,2	145,52
146,71	147,14	148,27	149,10,9,7	150,53	151,3	152,6,3,2	153,1
154,15	155,62	156,9	157,6,5,2	158,8,6,5	159,31	160,5,3,2	161,18
162,27	163,7,6,3	164,10,8,7	165,9,8,3	166,37	167,6	168,15,3,2	169,34
170,11	171,6,5,2	172,1	173,8,5,2	174,13	175,6	176,11,3,2	177,8
178,31	179,4,2,1	180,3	181,7,6,1	182,81	183,56	184,9,8,7	185,24
186,11	187,7,6,5	188,6,5,2	189,6,5,2	190,8,7,6	191,9	192,7,2,1	193,15
194,87	195,8,3,2	196,3	197,9,4,2	198,9	199,34	200,5,3,2	201,14
202,55	203,8,7,1	204,27	205,9,5,2	206,10,9,5	207,43	208,9,3,1	209,6
210,7	211,11,10,8	212,105	213,6,5,2	214,73	215,23	216,7,3,1	217,45
218,11	219,8,4,1	220,7	221,8,6,2	222,5,4,2	223,33	224,9,8,3	225,32
226,10,7,3	227,10,9,4	228,113	229,10,4,1	230,8,7,6	231,26	232,9,4,2	233,74
234,31	235,9,6,1	236,5	237,7,4,1	238,73	239,36	240,8,5,3	241,70
242,95	243,8,5,1	244,111	245,6,4,1	246,11,2,1	247,82	248,15,14,10	249,35
250,103	251,7,4,2	252,15	253,46	254,7,2,1	255,52	256,10,5,2	257,12
258,71	259,10,6,2	260,15	261,7,6,4	262,9,8,4	263,93	264,9,6,2	265,42
266,47	267,8,6,3	268,25	269,7,6,1	270,53	271,58	272,9,3,2	273,23
274,67	275,11,10,9	276,63	277,12,6,3	278,5	279,5	280,9,5,2	281,93
282,35	283,12,7,5	284,53	285,10,7,5	286,69	287,71	288,11,10,1	289,21
290,5,3,2	291,12,11,5	292,37	293,11,6,1	294,33	295,48	296,7,3,2	297,5
298,11,8,4	299,11,6,4	300,5	301,9,5,2	302,41	303,1	304,11,2,1	305,102
306,7,3,1	307,8,4,2	308,15	309,10,6,4	310,93	311,7,5,3	312,9,7,4	313,79
314,15	315,10,9,1	316,63	317,7,4,2	318,45	319,36	320,4,3,1	321,31
322,67	323,10,3,1	324,51	325,10,5,2	326,10,3,1	327,34	328,8,3,1	329,50
330,99	331,10,6,2	332,89	333,2	334,5,2,1	335,10,7,2	336,7,4,1	337,55
338,4,3,1	339,16,10,7	340,45	341,10,8,6	342,125	343,75	344,7,2,1	345,22
346,63	347,11,10,3	348,103	349,6,5,2	350,53	351,34	352,13,11,6	353,69
354,99	355,6,5,1	356,10,9,7	357,11,10,2	358,57	359,68	360,5,3,2	361,7,4,1
362,63	363,8,5,3	364,9	365,9,6,5	366,29	367,21	368,7,3,2	369,91
370,139	371,8,3,2	372,111	373,8,7,2	374,8,6,5	375,16	376,8,7,5	377,41
378,43	379,10,8,5	380,47	381,5,2,1	382,81	383,90	384,12,3,2	385,6
386,83	387,8,7,1	388,159	389,10,9,5	390,9	391,28	392,13,10,6	393,7
394,135	395,11,6,5	396,25	397,12,7,6	398,7,6,2	399,26	400,5,3,2	401,152
402,171	403,9,8,5	404,65	405,13,8,2	406,141	407,71	408,5,3,2	409,87
410,10,4,3	411,12,10,3	412,147	413,10,7,6	414,13	415,102	416,9,5,2	417,107
418,199	419,15,5,4	420,7	421,5,4,2	422,149	423,25	424,9,7,2	425,12
426,63	427,11,6,5	428,105	429,10,8,7	430,14,6,1	431,120	432,13,4,3	433,33
434,12,11,5	435,12,9,5	436,165	437,6,2,1	438,65	439,49	440,4,3,1	441,7
442,7,5,2	443,10,6,1	444,81	445,7,6,4	446,105	447,73	448,11,6,4	449,134
450,47	451,16,10,1	452,6,5,4	453,15,6,4	454,8,6,1	455,38	456,18,9,6	457,16
458,203	459,12,5,2	460,19	461,7,6,1	462,73	463,93	464,19,18,13	465,31
466,14,11,6	467,11,6,1	468,27	469,9,5,2	470,9	471,1	472,11,3,2	473,200
474,191	475,9,8,4	476,9	477,16,15,7	478,121	479,104	480,15,9,6	481,138

482,9,6,5	483,9,6,4	484,105	485,17,16,6	486,81	487,94	488,4,3,1	489,83
490,219	491,11,6,3	492,7	493,10,5,3	494,17	495,76	496,16,5,2	497,78
498,155	499,11,6,5	500,27	501,5,4,2	502,8,5,4	503,3	504,15,14,6	505,156
506,23	507,13,6,3	508,9	509,8,7,3	510,69	511,10	512,8,5,2	513,26
514,67	515,14,7,4	516,21	517,12,10,2	518,33	519,79	520,15,11,2	521,32
522,39	523,13,6,2	524,167	525,6,4,1	526,97	527,47	528,11,6,2	529,42
530,10,7,3	531,10,5,4	532,1	533,4,3,2	534,161	535,8,6,2	536,7,5,3	537,94
538,195	539,10,5,4	540,9	541,13,10,4	542,8,6,1	543,16	544,8,3,1	545,122
546,8,2,1	547,13,7,4	548,10,5,3	549,16,4,3	550,193	551,135	552,19,16,9	553,39
554,10,8,7	555,10,9,4	556,153	557,7,6,5	558,73	559,34	560,11,9,6	561,71
562,11,4,2	563,14,7,3	564,163	565,11,6,1	566,153	567,28	568,15,7,6	569,77
570,67	571,10,5,2	572,12,8,1	573,10,6,4	574,13	575,146	576,13,4,3	577,25
578,23,22,16	579,12,9,7	580,237	581,13,7,6	582,85	583,130	584,14,13,3	585,88
586,7,5,2	587,11,6,1	588,35	589,10,4,3	590,93	591,9,6,4	592,13,6,3	593,86
594,19	595,9,2,1	596,273	597,14,12,9	598,7,6,1	599,30	600,9,5,2	601,201
602,215	603,6,4,3	604,105	605,10,7,5	606,165	607,105	608,19,13,6	609,31
610,127	611,10,4,2	612,81	613,19,10,4	614,45	615,211	616,19,10,3	617,200
618,295	619,9,8,5	620,9	621,12,6,5	622,297	623,68	624,11,6,5	625,133
626,251	627,13,8,4	628,223	629,6,5,2	630,7,4,2	631,307	632,9,2,1	633,101
634,39	635,14,10,4	636,217	637,14,9,1	638,6,5,1	639,16	640,14,3,2	641,11
642,119	643,11,3,2	644,11,6,5	645,11,8,4	646,249	647,5	648,13,3,1	649,37
650,3	651,14	652,93	653,10,8,7	654,33	655,88	656,7,5,4	657,38
658,55	659,15,4,2	660,11	661,12,11,4	662,21	663,107	664,11,9,8	665,33
666,10,7,2	667,18,7,3	668,147	669,5,4,2	670,153	671,15	672,11,6,5	673,28
674,11,7,4	675,6,3,1	676,31	677,8,4,3	678,15,5,3	679,66	680,23,16,9	681,11,9,3
682,171	683,11,6,1	684,209	685,4,3,1	686,197	687,13	688,19,14,6	689,14
690,79	691,13,6,2	692,299	693,15,8,2	694,169	695,177	696,23,10,2	697,267
698,215	699,15,10,1	700,75	701,16,4,2	702,37	703,12,7,1	704,8,3,2	705,17
706,12,11,8	707,15,8,5	708,15	709,4,3,1	710,13,12,4	711,92	712,5,4,3	713,41
714,23	715,7,4,1	716,183	717,16,7,1	718,165	719,150	720,9,6,4	721,9
722,231	723,16,10,4	724,207	725,9,6,5	726,5	727,180	728,4,3,2	729,58
730,147	731,8,6,2	732,343	733,8,7,2	734,11,6,1	735,44	736,13,8,6	737,5
738,347	739,18,16,8	740,135	741,9,8,3	742,85	743,90	744,13,11,1	745,258
746,351	747,10,6,4	748,19	749,7,6,1	750,309	751,18	752,13,10,3	753,158
754,19	755,12,10,1	756,45	757,7,6,1	758,233	759,98	760,11,6,5	761,3
762,83	763,16,14,9	764,6,5,3	765,9,7,4	766,22,19,9	767,168	768,19,17,4	769,120
770,14,5,2	771,17,15,6	772,7	773,10,8,6	774,185	775,93	776,15,14,7	777,29
778,375	779,10,8,3	780,13	781,17,16,2	782,329	783,68	784,13,9,6	785,92
786,12,10,3	787,7,6,3	788,17,10,3	789,5,2,1	790,9,6,1	791,30	792,9,7,3	793,253
794,143	795,7,4,1	796,9,4,1	797,12,10,4	798,53	799,25	800,9,7,1	801,217
802,15,13,9	803,14,9,2	804,75	805,8,7,2	806,21	807,7	808,14,3,2	809,15
810,159	811,12,10,8	812,29	813,10,3,1	814,21	815,333	816,11,8,2	817,52
818,119	819,16,9,7	820,123	821,15,11,2	822,17	823,9	824,11,6,4	825,38
826,255	827,12,10,7	828,189	829,4,3,1	830,17,10,7	831,49	832,13,5,2	833,149
834,15	835,14,7,5	836,10,9,2	837,8,6,5	838,61	839,54	840,11,5,1	841,144
842,47	843,11,10,7	844,105	845,2	846,105	847,136	848,11,4,1	849,253
850,111	851,13,10,5	852,159	853,10,7,1	854,7,5,3	855,29	856,19,10,3	857,119
858,207	859,17,15,4	860,35	861,14	862,349	863,6,3,2	864,21,10,6	865,1
866,75	867,9,5,2	868,145	869,11,7,6	870,301	871,378	872,13,3,1	873,352
874,12,7,4	875,12,8,1	876,149	877,6,5,4	878,12,9,8	879,11	880,15,7,5	881,78
882,99	883,17,16,12	884,173	885,8,7,1	886,13,9,8	887,147	888,19,18,10	889,127
890,183	891,12,4,1	892,31	893,11,8,6	894,173	895,12	896,7,5,3	897,113
898,207	899,18,15,5	900,1	901,13,7,6	902,21	903,35	904,12,7,2	905,117
906,123	907,12,10,2	908,143	909,14,4,1	910,15,9,7	911,204	912,7,5,1	913,91
914,4,2,1	915,8,6,3	916,183	917,12,10,7	918,77	919,36	920,14,9,6	921,221
922,7,6,5	923,16,14,13	924,31	925,16,15,7	926,365	927,403	928,10,3,2	929,11,4,3
930,31	931,10,9,4	932,177	933,16,6,1	934,22,6,5	935,417	936,15,13,12	937,217
938,207	939,7,5,4	940,10,7,1	941,11,6,1	942,45	943,24	944,12,11,9	945,77
946,21,20,13	947,9,6,5	948,189	949,8,3,2	950,13,12,10	951,260	952,16,9,7	953,168
954,131	955,7,6,3	956,305	957,10,9,6	958,13,9,4	959,143	960,12,9,3	961,18
962,15,8,5	963,20,9,6	964,103	965,15,4,2	966,201	967,36	968,9,5,2	969,31
970,11,7,2	971,6,2,1	972,7	973,13,6,4	974,9,8,7	975,19	976,17,10,6	977,15
978,9,3,1	979,178	980,8,7,6	981,12,6,5	982,177	983,230	984,24,9,3	985,222
986,3	987,16,13,12	988,121	989,10,4,2	990,161	991,39	992,17,15,13	993,62
994,223	995,15,12,2	996,65	997,12,6,3	998,101	999,59	1000,5,4,3	1001,17
1002,5,3,2	1003,13,8,3	1004,10,9,7	1005,12,8,2	1006,5,4,3	1007,75	1008,19,17,8	1009,55
1010,99	1011,10,7,4	1012,115	1013,9,8,6	1014,385	1015,186	1016,15,6,3	1017,9,4,1
1018,12,10,5	1019,10,8,1	1020,135	1021,5,2,1	1022,317	1023,7	1024,19,6,1	1025,294

Table 2.2.1 Lowest weight lowest-lexicographical order irreducible polynomial of degree n over $\mathbb{F}_2$. Output: n, k (for trinomials $x^n + x^k + 1$) or n, k_1, k_2, k_3 (for pentanomials $x^n + x^{k_1} + x^{k_2} + x^{k_3} + 1$).

2.2.4 Remark Constructions of irreducible low-weight polynomials are rare; see Sections 3.4 and 3.5. Instead, conditions for reducibility are often more tractable; see Section 3.3. Swan [2753] gives conditions for when a trinomial $x^n + x^k + 1 \in \mathbb{F}_2[x]$ is reducible. In particular, the trinomial is reducible when 8 divides n. Only partial results for Swan-like

conditions on pentanomials over $\mathbb{F}_2$ exist in the literature; see, for example, [1777] and Section 3.3.

2.2.5 Conjecture [2582] For every n, there exists either an irreducible trinomial of degree n over $\mathbb{F}_2$ or, in the absence of an irreducible trinomial, there exists an irreducible pentanomial of degree n over $\mathbb{F}_2$.

2.2.6 Remark A polynomial over $\mathbb{F}_q$ is *primitive* if all of its roots are generators of the (cyclic) multiplicative group $\mathbb{F}_q^*$. We give an analogous table to Table 2.2.1 but instead list the lowest-weight lowest-lexicographical order primitive polynomial of degree $n \leq 577$ over $\mathbb{F}_2$. To compute primitivity, we used the *Cunningham project* to find the factorization of $2^n - 1$; see Section 2.2.3 for more details.

2,1	3,1	4,1	5,2	6,1	7,1	8,4,3,2	9,4
10,3	11,2	12,6,4,1	13,4,3,1	14,5,3,1	15,1	16,5,3,2	17,3
18,7	19,5,2,1	20,3	21,2	22,1	23,5	24,4,3,1	25,3
26,6,2,1	27,5,2,1	28,3	29,2	30,6,4,1	31,3	32,7,6,2	33,13
34,8,4,3	35,2	36,11	37,6,4,1	38,6,5,1	39,4	40,5,4,3	41,3
42,7,4,3	43,6,4,3	44,6,5,2	45,4,3,1	46,8,7,6	47,5	48,9,7,4	49,9
50,4,3,2	51,6,3,1	52,3	53,6,2,1	54,8,6,3	55,24	56,7,4,2	57,7
58,19	59,7,4,2	60,1	61,5,2,1	62,6,5,3	63,1	64,4,3,1	65,18
66,9,8,6	67,5,2,1	68,9	69,6,5,2	70,5,3,1	71,6	72,10,9,3	73,25
74,7,4,3	75,6,3,1	76,5,4,2	77,6,5,2	78,7,2,1	79,9	80,9,4,2	81,4
82,9,6,4	83,7,4,2	84,13	85,8,2,1	86,6,5,2	87,13	88,11,9,8	89,38
90,5,3,2	91,8,5,1	92,6,5,2	93,2	94,21	95,11	96,10,9,6	97,6
98,11	99,7,5,4	100,37	101,7,6,1	102,6,5,3	103,9	104,11,10,1	105,16
106,15	107,9,7,4	108,31	109,5,4,2	110,6,4,1	111,10	112,11,6,4	113,9
114,11,2,1	115,8,7,5	116,6,5,2	117,5,2,1	118,33	119,8	120,9,6,2	121,18
122,6,2,1	123,2	124,37	125,7,6,5	126,7,4,2	127,1	128,7,2,1	129,5
130,3	131,8,3,2	132,29	133,9,8,2	134,57	135,11	136,8,3,2	137,21
138,8,7,1	139,8,5,3	140,29	141,13,6,1	142,21	143,5,3,2	144,7,4,2	145,52
146,5,3,2	147,11,4,2	148,27	149,10,9,7	150,53	151,3	152,6,3,2	153,1
154,9,5,1	155,7,5,4	156,9,5,3	157,6,5,2	158,8,6,5	159,31	160,5,3,2	161,18
162,8,7,4	163,7,6,3	164,12,6,5	165,9,8,3	166,10,3,2	167,6	168,16,9,6	169,34
170,23	171,6,5,2	172,7	173,8,5,2	174,13	175,6	176,12,11,9	177,8
178,87	179,4,2,1	180,12,10,7	181,7,6,1	182,8,6,1	183,56	184,9,8,7	185,24
186,9,8,6	187,7,6,5	188,6,5,2	189,6,5,2	190,13,6,2	191,9	192,15,11,5	193,15
194,87	195,8,3,2	196,11,9,2	197,9,4,2	198,65	199,34	200,5,3,2	201,14
202,55	203,8,7,1	204,10,4,3	205,9,5,2	206,10,9,5	207,43	208,9,3,1	209,6
210,12,4,3	211,11,10,8	212,105	213,6,5,2	214,5,3,1	215,23	216,7,3,1	217,45
218,11	219,8,4,1	220,12,10,9	221,8,6,2	222,8,5,2	223,33	224,12,7,2	225,32
226,10,7,3	227,10,9,4	228,12,11,2	229,10,4,1	230,8,7,6	231,26	232,11,9,4	233,74
234,31	235,9,6,1	236,5	237,7,4,1	238,5,2,1	239,36	240,8,5,3	241,70
242,11,6,1	243,8,5,1	244,9,4,1	245,6,4,1	246,11,2,1	247,82	248,15,14,10	249,86
250,103	251,7,4,2	252,67	253,7,3,2	254,7,2,1	255,52	256,10,5,2	257,12
258,83	259,10,6,2	260,10,8,7	261,7,6,4	262,9,8,4	263,93	264,10,9,1	265,42
266,47	267,8,6,3	268,25	269,7,6,1	270,53	271,58	272,9,6,2	273,23
274,67	275,11,10,9	276,6,3,1	277,12,6,3	278,5	279,5	280,9,5,2	281,93
282,35	283,12,7,5	284,119	285,10,7,5	286,69	287,71	288,11,10,1	289,21
290,5,3,2	291,12,11,5	292,97	293,11,6,1	294,61	295,48	296,11,9,4	297,5
298,11,8,4	299,11,6,4	300,7	301,9,5,2	302,41	303,13,12,6	304,11,2,1	305,102
306,7,3,1	307,8,4,2	308,15,9,2	309,10,6,4	310,8,5,1	311,7,5,3	312,11,10,5	313,79
314,15	315,10,9,1	316,135	317,7,4,2	318,8,6,5	319,36	320,4,3,1	321,31
322,67	323,10,3,1	324,6,4,3	325,10,5,2	326,10,3,1	327,34	328,9,7,5	329,50
330,8,7,2	331,10,6,2	332,123	333,2	334,7,4,1	335,10,7,2	336,7,4,1	337,55
338,6,3,2	339,16,10,7	340,11,4,3	341,14,11,5	342,125	343,75	344,11,10,6	345,22
346,11,7,2	347,11,10,3	348,8,7,4	349,6,5,2	350,53	351,34	352,13,11,6	353,69
354,14,13,5	355,6,5,1	356,10,9,7	357,11,10,2	358,14,8,7	359,68	360,26,25,1	361,7,4,1
362,63	363,8,5,3	364,67	365,9,6,5	366,29	367,21	368,17,9,7	369,91
370,139	371,8,3,2	372,15,7,3	373,8,7,2	374,8,6,5	375,16	376,8,7,5	377,41
378,43	379,10,8,5	380,47	381,5,2,1	382,81	383,90	384,16,15,6	385,6
386,83	387,9,8,2	388,14,3,1	389,10,9,5	390,89	391,28	392,13,10,6	393,7
394,135	395,11,6,5	396,25	397,12,7,6	398,14,6,5	399,86	400,5,3,2	401,152
402,9,4,3	403,9,8,5	404,189	405,17,8,7	406,157	407,71	408,7,5,1	409,87
410,10,4,3	411,12,10,3	412,147	413,10,7,6	414,16,13,9	415,102	416,9,5,2	417,107
418,15,3,1	419,15,5,4	420,13,10,8	421,5,4,2	422,149	423,25	424,9,7,2	425,12
426,14,12,11	427,11,6,5	428,105	429,10,8,7	430,15,13,11	431,120	432,13,4,3	433,33
434,12,11,5	435,12,9,5	436,165	437,6,2,1	438,65	439,49	440,4,3,1	441,31

442,7,5,2	443,10,6,1	444,13,12,9	445,7,6,4	446,105	447,73	448,11,6,4	449,134
450,79	451,16,10,1	452,6,5,4	453,15,6,4	454,10,9,5	455,38	456,23,11,2	457,16
458,203	459,12,5,2	460,61	461,7,6,1	462,73	463,93	464,23,9,4	465,59
466,14,11,6	467,11,6,1	468,15,9,4	469,9,5,2	470,149	471,1	472,11,3,2	473,8,6,3
474,191	475,9,8,4	476,15	477,16,15,7	478,121	479,104	480,16,13,7	481,138
482,9,6,5	483,9,6,4	484,105	485,17,16,6	486,14,8,5	487,94	488,4,3,1	489,83
490,219	491,11,6,3	492,8,7,1	493,10,5,3	494,137	495,76	496,16,5,2	497,78
498,11,9,3	499,11,6,5	500,10,6,1	501,5,4,2	502,8,5,4	503,3	504,21,14,2	505,156
506,95	507,13,6,3	508,109	509,8,7,3	510,12,10,9	511,10	512,8,5,2	513,85
514,7,5,3	515,14,7,4	516,7,5,2	517,12,10,2	518,33	519,79	520,17,13,11	521,32
522,15,13,4	523,13,6,2	524,167	525,6,4,1	526,9,5,1	527,47	528,11,6,2	529,42
530,10,7,3	531,12,6,2	532,1	533,4,3,2	534,7,5,1	535,8,6,2	536,7,5,3	537,94
538,5,2,1	539,10,5,4	540,179	541,13,10,4	542,9,3,2	543,16	544,13,9,6	545,122
546,8,2,1	547,13,7,4	548,10,5,3	549,16,4,3	550,193	551,135	552,20,5,2	553,39
554,11,8,3	555,10,9,4	556,153	557,7,6,5	558,14,9,5	559,34	560,11,9,6	561,71
562,11,4,2	563,14,7,3	564,163	565,11,6,1	566,153	567,143	568,17,11,10	569,77
570,67	571,10,5,2	572,12,8,1	573,10,6,4	574,13	575,146	576,13,4,3	577,25

Table 2.2.2 Lowest weight lowest-lexicographical order primitive polynomial of degree $n \leq 577$ over $\mathbb{F}_2$. Output: n, k (for trinomials $x^n + x^k + 1$) or n, k_1, k_2, k_3 (for pentanomials $x^n + x^{k_1} + x^{k_2} + x^{k_3} + 1$).

2.2.7 Remark Table 2.2.3 is the analogous table to Table 2.2.1, giving the lowest-weight, lowest-lexicographical order irreducible polynomial of degree $n \leq 516$ over $\mathbb{F}_3$.

2,(1)	3,1(2),(1)	4,1(1),(2)	5,1(2),(1)	6,1(1),(2)
7,2(1),(2)	8,2(1),(2)	9,4(1),(2)	10,2(2),(1)	11,2(1),(2)
12,2(1),(2)	13,1(2),(1)	14,1(1),(2)	15,2(1),(2)	16,4(1),(2)
17,1(2),(1)	18,7(1),(2)	19,2(1),(2)	20,5(1),(2)	21,5(2),(1)
22,4(2),(1)	23,3(2),(1)	24,4(1),(2)	25,3(2),(1)	26,2(2),(1)
27,7(2),(1)	28,2(1),(2)	29,4(1),(2)	30,1(1),(2)	31,5(2),(1)
32,5(1),(2)	33,5(2),(1)	34,2(2),(1)	35,2(1),(2)	36,14(1),(2)
37,6(1),(2)	38,4(2),(1)	39,7(2),(1)	40,1(1),(2)	41,1(2),(1)
42,7(1),(2)	43,17(2),(1)	44,3(1),(2)	45,17(2),(1)	46,5(1),(2)
47,15(2),(1)	48,8(1),(2)	49,3(2),2(1),(1)	50,6(2),(1)	51,1(2),(1)
52,7(1),(2)	53,13(2),(1)	54,1(1),(2)	55,11(2),(1)	56,3(1),(2)
57,7(1),2(1),(2)	58,8(2),(1)	59,17(2),(1)	60,2(1),(2)	61,7(2),(1)
62,10(2),(1)	63,26(1),(2)	64,3(1),(2)	65,5(1),3(1),(1)	66,10(2),(1)
67,2(1),(2)	68,3(1),2(1),(1)	69,17(2),(1)	70,4(2),(1)	71,20(1),(2)
72,28(1),(2)	73,1(2),(1)	74,12(2),(1)	75,5(2),4(1),(1)	76,9(1),(2)
77,16(1),(2)	78,13(1),(2)	79,26(1),(2)	80,2(1),(2)	81,40(1),(2)
82,2(2),(1)	83,27(2),(1)	84,14(1),(2)	85,16(1),(2)	86,13(1),(2)
87,26(1),(2)	88,6(1),(2)	89,13(2),(1)	90,19(1),(2)	91,17(2),(1)
92,10(1),(2)	93,23(2),(1)	94,30(2),(1)	95,47(2),(1)	96,16(1),(2)
97,12(1),(2)	98,4(1),3(1),(1)	99,19(2),(1)	100,25(1),(2)	101,31(2),(1)
102,2(2),(1)	103,47(2),(1)	104,5(1),(2)	105,6(1),2(1),(1)	106,26(2),(1)
107,3(2),(1)	108,2(1),(2)	109,9(2),(1)	110,22(2),(1)	111,2(1),(2)
112,6(1),(2)	113,19(2),(1)	114,7(1),(2)	115,32(1),(2)	116,15(1),(2)
117,52(1),(2)	118,34(2),(1)	119,2(1),(2)	120,4(1),(2)	121,1(2),(1)
122,14(2),(1)	123,7(1),4(1),(2)	124,25(1),(2)	125,52(1),(2)	126,49(1),(2)
127,8(1),(2)	128,6(1),(2)	129,3(2),2(1),(1)	130,10(1),6(1),(1)	131,27(2),(1)
132,19(1),14(1),(1)	133,15(2),(1)	134,4(2),(1)	135,44(1),(2)	136,57(1),(2)
137,1(2),(1)	138,34(2),(1)	139,59(2),(1)	140,59(1),(2)	141,5(2),(1)
142,40(2),(1)	143,35(2),(1)	144,56(1),(2)	145,24(1),(2)	146,2(2),(1)
147,8(1),(2)	148,3(1),(2)	149,11(2),10(1),(1)	150,73(1),(2)	151,2(1),(2)
152,18(1),(2)	153,59(2),(1)	154,32(2),(1)	155,12(1),(2)	156,26(1),(2)
157,22(1),(2)	158,52(2),(1)	159,32(1),(2)	160,4(1),(2)	161,9(1),5(1),(1)
162,19(1),(2)	163,59(2),(1)	164,15(1),(2)	165,22(1),(2)	166,54(2),(1)
167,71(2),(1)	168,28(1),(2)	169,24(1),(2)	170,32(2),(1)	171,20(1),(2)
172,19(1),(2)	173,7(2),(1)	174,52(2),(1)	175,10(1),8(1),(1)	176,12(1),(2)
177,52(1),(2)	178,11(1),(2)	179,59(2),(1)	180,38(1),(2)	181,37(2),(1)
182,25(1),(2)	183,2(1),(2)	184,20(1),(2)	185,64(1),(2)	186,46(2),(1)
187,8(1),(2)	188,11(1),(2)	189,9(1),7(1),(1)	190,94(2),(1)	191,71(2),(1)
192,32(1),(2)	193,12(1),(2)	194,24(2),(1)	195,26(1),(2)	196,79(1),(2)
197,9(1),7(1),(1)	198,29(1),(2)	199,35(2),(1)	200,3(1),(2)	201,88(1),(2)
202,62(2),(1)	203,3(2),(1)	204,50(1),(2)	205,9(2),(1)	206,61(1),(2)
207,11(2),8(1),(1)	208,10(1),(2)	209,40(1),(2)	210,7(1),(2)	211,89(2),(1)
212,14(1),3(1),(1)	213,17(2),4(1),(1)	214,6(2),(1)	215,36(1),(2)	216,4(1),(2)
217,85(2),(1)	218,18(2),(1)	219,25(2),(1)	220,15(1),(2)	221,12(1),2(1),(1)
222,4(2),(1)	223,8(1),5(2),(1)	224,12(1),(2)	225,16(1),(2)	226,38(2),(1)
227,11(2),(1)	228,14(1),(2)	229,72(1),(2)	230,64(2),(1)	231,8(1),7(1),(2)
232,30(1),(2)	233,6(1),2(1),(1)	234,91(1),(2)	235,26(1),(2)	236,9(1),(2)
237,70(1),(2)	238,4(2),(1)	239,5(2),(1)	240,8(1),(2)	241,88(1),(2)
242,2(2),(1)	243,121(2),(1)	244,31(1),(2)	245,97(2),(1)	246,13(1),(2)
247,122(1),(2)	248,50(1),(2)	249,59(2),(1)	250,104(2),(1)	251,9(2),(1)
252,98(1),(2)	253,7(2),(1)	254,16(2),(1)	255,26(1),(2)	256,12(1),(2)

257,22(1),(2)	258,7(1),(2)	259,65(2),(1)	260,35(1),(2)	261,119(2),(1)
262,54(2),(1)	263,69(2),(1)	264,23(1),16(1),(1)	265,61(2),(1)	266,30(2),(1)
267,9(1),2(1),(2)	268,15(1),(2)	269,7(2),(1)	270,88(2),(1)	271,50(1),(2)
272,114(1),(2)	273,46(1),(2)	274,2(2),(1)	275,12(1),(2)	276,10(1),2(1),(2)
277,24(1),(2)	278,118(2),(1)	279,7(2),(1)	280,15(1),(2)	281,10(1),7(1),(2)
282,10(2),(1)	283,23(2),(1)	284,5(1),(2)	285,89(2),(1)	286,70(2),(1)
287,101(2),(1)	288,112(1),(2)	289,73(2),(1)	290,43(1),(2)	291,25(2),(1)
292,13(1),12(1),(1)	293,7(2),(1)	294,16(2),(1)	295,83(2),(1)	296,6(1),(2)
297,3(2),2(1),(1)	298,13(1),3(1),(2)	299,51(2),(1)	300,146(1),(2)	301,30(1),(2)
302,4(2),(1)	303,8(1),2(1),(1)	304,36(1),(2)	305,46(1),(2)	306,118(2),(1)
307,17(2),(1)	308,53(1),(2)	309,3(2),2(1),(1)	310,24(2),(1)	311,13(2),12(1),(1)
312,52(1),(2)	313,93(2),(1)	314,44(2),(1)	315,127(2),(1)	316,87(1),(2)
317,7(2),(1)	318,64(2),(1)	319,10(1),9(1),(2)	320,3(1),(2)	321,83(2),(1)
322,71(1),(2)	323,9(2),(1)	324,38(1),(2)	325,157(2),(1)	326,118(2),(1)
327,7(2),(1)	328,3(1),(2)	329,52(1),(2)	330,11(1),(2)	331,2(1),(2)
332,13(1),6(1),(1)	333,94(1),(2)	334,142(2),(1)	335,8(1),(2)	336,56(1),(2)
337,3(2),(1)	338,48(2),(1)	339,49(2),(1)	340,86(1),(2)	341,25(2),(1)
342,40(2),(1)	343,12(1),10(1),(1)	344,38(1),(2)	345,101(2),(1)	346,14(2),(1)
347,18(1),(2)	348,146(1),(2)	349,54(1),(2)	350,157(1),(2)	351,20(1),(2)
352,7(1),(2)	353,142(1),(2)	354,104(2),(1)	355,41(2),(1)	356,15(1),(2)
357,71(2),(1)	358,77(1),(2)	359,15(2),(1)	360,76(1),(2)	361,157(2),(1)
362,74(2),(1)	363,26(1),(2)	364,1(1),(2)	365,88(1),(2)	366,4(2),(1)
367,107(2),(1)	368,27(1),(2)	369,11(2),(1)	370,11(1),(2)	371,27(2),(1)
372,94(1),(2)	373,25(2),(1)	374,16(2),(1)	375,67(2),(1)	376,9(1),(2)
377,160(1),(2)	378,7(1),(2)	379,44(1),(2)	380,9(1),(2)	381,143(2),(1)
382,137(1),(2)	383,80(1),(2)	384,64(1),(2)	385,22(1),(2)	386,24(2),(1)
387,152(1),(2)	388,87(1),(2)	389,76(1),(2)	390,13(1),(2)	391,22(1),21(2),(1)
392,158(1),(2)	393,185(2),(1)	394,14(1),9(1),(1)	395,23(2),(1)	396,58(1),(2)
397,12(1),5(1),(2)	398,70(2),(1)	399,181(2),(1)	400,3(1),(2)	401,11(2),10(1),(1)
402,176(2),(1)	403,161(2),(1)	404,9(1),2(1),(1)	405,25(1),18(1),(2)	406,6(2),(1)
407,48(1),(2)	408,100(1),(2)	409,99(2),(1)	410,18(2),(1)	411,8(1),2(1),(1)
412,79(1),(2)	413,22(1),(2)	414,37(1),(2)	415,13(1),3(1),(1)	416,20(1),(2)
417,40(1),(2)	418,80(2),(1)	419,26(1),(2)	420,14(1),(2)	421,13(2),(1)
422,178(2),(1)	423,68(1),(2)	424,45(1),(2)	425,61(2),(1)	426,9(1),7(1),(2)
427,167(2),(1)	428,71(1),(2)	429,65(2),(1)	430,72(2),(1)	431,66(1),(2)
432,8(1),(2)	433,120(1),(2)	434,67(1),(2)	435,8(1),2(1),(1)	436,13(1),2(1),(1)
437,14(1),3(2),(1)	438,17(1),(2)	439,16(1),3(2),(1)	440,11(1),(2)	441,7(1),6(1),(2)
442,11(1),3(1),(2)	443,188(1),(2)	444,178(1),(2)	445,141(2),(1)	446,1(1),(2)
447,157(2),(1)	448,24(1),(2)	449,52(1),(2)	450,32(2),(1)	451,17(2),(1)
452,17(1),(2)	453,17(2),4(1),(1)	454,22(2),(1)	455,32(1),(2)	456,28(1),(2)
457,67(2),(1)	458,144(2),(1)	459,13(2),6(1),(1)	460,57(1),(2)	461,13(2),(1)
462,73(1),(2)	463,15(1),13(1),(1)	464,60(1),(2)	465,41(2),(1)	466,167(1),(2)
467,48(1),(2)	468,182(1),(2)	469,166(1),(2)	470,52(2),(1)	471,8(1),(2)
472,18(1),(2)	473,73(2),(1)	474,83(1),(2)	475,17(2),(1)	476,10(1),(2)
477,101(2),(1)	478,10(2),(1)	479,221(2),(1)	480,16(1),(2)	481,22(1),(2)
482,127(1),(2)	483,26(1),(2)	484,39(1),(2)	485,1(2),(1)	486,125(1),(2)
487,29(2),(1)	488,62(1),(2)	489,7(1),5(1),(1)	490,194(2),(1)	491,11(2),(1)
492,26(1),(2)	493,4(1),(2)	494,244(2),(1)	495,7(2),(1)	496,85(1),(2)
497,7(2),6(1),(1)	498,118(2),(1)	499,20(1),(2)	500,39(1),(2)	501,88(1),(2)
502,18(2),(1)	503,35(2),(1)	504,196(1),(2)	505,61(2),(1)	506,14(2),(1)
507,80(1),(2)	508,91(1),(2)	509,151(2),(1)	510,52(2),(1)	511,215(2),(1)
512,24(1),(2)	513,14(1),10(1),(1)	514,44(2),(1)	515,8(1),(2)	516,14(1),(2)

Table 2.2.3 Lowest weight lowest lexicographical order irreducible polynomial of degree n over $\mathbb{F}_3$. Output: n, {*degrees, (coefficients)*}, *(constant term)*.

2.2.8 Remark Necessary and sufficient conditions for the existence of an irreducible binomial of degree n over finite fields of odd characteristic are given in [1939, Theorem 3.75]. A constructive derivation of the degrees for which there exists an irreducible binomial over $\mathbb{F}_q$, q odd, is given in [2356]. The following conjecture summarizes empirical observations of extending Tables 2.2.1 and 2.2.3 to higher characteristics.

2.2.9 Conjecture Let $q > 2$. For every n, there is an irreducible polynomial of degree n over $\mathbb{F}_q$ of weight at most 4.

2.2.2 Low-complexity normal bases

2.2.10 Remark Normal bases are often required in hardware implementations of finite fields due to the efficiency of exponentiation when the finite field is represented using a normal basis.

The *complexity* of a normal basis N, C_N, is defined in Definition 5.3.1. Normal bases with low complexity are highly preferred. An *optimal* normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is a normal basis attaining the minimum complexity $C_N = 2n - 1$. See Sections 5.2 and 5.3 for more details on normal bases and their complexities.

2.2.2.1 Exhaustive search for low complexity normal bases

2.2.11 Remark Table 2.2.4 is due to an exhaustive search for normal bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, $n \leq 39$, originally given in [2015]. The table gives the number of normal bases, the smallest and largest complexities (m_{C_N}, M_{C_N}), the average and variance (Avg_{C_N}, Var_{C_N}) of complexities and the smallest and largest complexities for self-dual normal elements. In Table 2.2.4, we fix a typo on the minimum complexity of $n = 37$, originally noted in [130], and make some minor corrections to the calculations of the averages and variances. In the "Notes" column, "Optimal" indicates that the basis with minimal complexity is an optimal normal basis (Theorem 5.3.6), and "sd" indicates that the minimal complexity basis is self-dual.

						Self-dual		
n	# Normal bases	m_{C_N}	M_{C_N}	Avg_{C_N}	Var_{C_N}	m_{C_N}	M_{C_N}	Notes
2	1	3	3	3.00	0	3	3	Optimal, sd
3	1	5	5	5.00	0	5	5	Optimal, sd
4	2	7	9	8.00	1.00	-	-	
5	3	9	15	11.67	6.22	9	9	Optimal, sd
6	4	11	17	15.00	6.00	11	15	Optimal, sd
7	7	19	27	23.00	9.14	21	21	$m_{C_N} = 3n - 2$
8	16	21	35	29.00	11	-	-	$m_{C_N} = 3n - 3$
9	21	17	45	35.57	41.57	17	29	Optimal, sd
10	48	19	61	44.83	61.31	27	51	
11	93	21	71	55.82	57.65	21	57	Optimal, sd
12	128	23	83	64.13	107.23	-	-	
13	315	45	101	78.38	71.07	45	81	sd
14	448	27	135	91.07	108.42	27	135	Optimal, sd
15	675	45	137	105.89	127.36	45	105	sd
16	2048	85	157	115.82	114.59	-	-	
17	3825	81	177	136.83	136.67	81	171	sd
18	5376	35	243	153.51	185.12	35	243	Optimal, sd
19	13797	117	229	172.00	171.91	117	201	sd
20	24576	63	257	190.81	205.81	-	-	
21	27783	95	277	210.97	216.43	105	237	
22	95232	63	363	231.93	238.56	63	363	$m_{C_N} = 3n - 3$
23	182183	45	325	254.02	254.60	45	309	Optimal, sd
24	262144	105	375	276.89	281.01	-	-	
25	629145	93	383	301.01	300.37	93	357	sd
26	1290240	51	555	325.96	328.59	51	555	Optimal, sd
27	1835001	141	443	351.99	351.38	141	413	
28	3670016	55	517	378.98	379.12	-	-	Optimal
29	9256395	57	521	407.00	406.21	57	465	Optimal, sd
30	11059200	59	759	435.95	438.52	59	759	Optimal, sd
31	28629151	237	587	466.00	465.21	237	537	sd
32	67108864	361	621	497.00	496.07	-	-	
33	97327197	65	693	529.00	528.44	65	693	Optimal, sd
34	250675200	243	819	562.00	561.52	243	819	sd
35	352149515	69	779	596.00	595.08	69	693	Optimal, sd
36	704643060	71	1017	630.99	630.51	-	-	Optimal
37	1857283155	141	823	667	666.04	141		sd
38	3616800703	207	1131	704.00	703.18	207		
39	5282242828	77	933	742.00	741.09	77		Optimal, sd

Table 2.2.4 Statistics for normal bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ obtained by exhaustive search, $n \leq 39$.

2.2.12 Remark Our first conjecture based on Table 2.2.4 appears in [3036] and elsewhere. We also summarize the conjectures found in [2015].

2.2.13 Conjecture When no optimal normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ exists, the minimum complexity of a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ is $3n - 3$.

2.2.14 Remark Normal bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ achieving a complexity of $3n-3$ are given in Proposition 5.3.46 and this complexity is the minimal found when $n=8$ and $n=22$.

2.2.15 Conjecture The number of normal bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ are normally distributed with respect to their complexities. Furthermore, the average complexity of a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ is $(n^2-n+3)/2$ and the variance is also $n^2/2-cn$, for a small positive constant c.

2.2.16 Remark We remark that the conspicuous wording in Conjecture 2.2.15, that normal bases are normally distributed, is mostly coincidental. Indeed, as n grows, the number of normal bases grow like $2^n/\log(n)$, see Theorem 5.2.13, so the Central Limit Theorem supports this conjecture. The precise distribution of the complexities is still an open and interesting problem.

2.2.17 Remark Self-dual normal bases are often preferred in normal basis implementations due to their highly symmetric properties; see Sections 5.1, 5.2, 5.3, 16.7 as well as [1264, 2925], for more information on self-dual normal bases and their implementations. Exhaustive searches of self-dual normal bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ appear in [130, 1263, 1631, 2015] and [130] gives an exhastive search of self-dual normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ for larger q and odd n. Tables 2.2.5, 2.2.6, and 2.2.7 are directly from [130]; we note that we did not implement their algorithm. Table 2.2.5 gives the minimum complexity C_n of a self-dual normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ for odd $n \le 45$, Table 2.2.6 for q a power of 2 and small n, and Table 2.2.7 for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ for odd $q \le 19$ and small n.

n	3	5	7	9	11	13	15	17	19	21	23
C_n	5	9	21	17	21	45	45	81	117	105	45

n	25	27	29	31	33	35	37	39	41	43	45
C_n	93	141	57	237	65	69	141	77	81	165	153

Table 2.2.5 The lowest complexity for self-dual normal bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ for odd n, $n \le 45$.

q/n	3	5	7	9	11	13	15	17	19	21	23	25
2	5	9	21	17	21	45	45	81	117	105	45	93
4	5	9	21	17	21	45	45	81	117	105	45	93
8	9	9	21	45	21	45	81	81				
16	5	9	21	17	21	45						
32	5	19	21	17	21							
64	9	9	21	45								
128	5	9	37									
256	5	9										

Table 2.2.6 Lowest complexity for self-dual normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ where q is a power of 2 for small odd values of n.

q/n	3	5	7	9	11	13	15	17	19	21	23	25
3	7	13	25	37	55	67	–	91	172	–	127	135
5	6	13	25	46	64	85	–	157	153	150		
7	6	16	19	41	61	96	87			–		
11	6	13	25	52	31	100	78					
13	6	13	25	51	64	37						
17	8	13	25	51	64	100		–				
19	8	13	31	51	67				–			

Table 2.2.7 Lowest complexity for self-dual normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ for odd primes $q \le 19$ and small odd values of n.

2.2.2.2 Minimum type of a Gauss period admitting a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$

2.2.18 Remark We briefly recall the definition of a Gauss period (Definition 5.3.16). Let $r = nk+1$ be a prime not dividing q and let γ be a primitive r-th root of unity in $\mathbb{F}_{q^{nk}}$. Furthermore, let K be the unique subgroup of order k in $\mathbb{Z}_r^*$ and $K_i = \{a \cdot q^i : a \in K\} \subseteq \mathbb{Z}_r^*$ be cosets of K, $0 \leq i \leq n-1$. The elements

$$\alpha_i = \sum_{a \in K_i} \gamma^a \in \mathbb{F}_{q^n}, \quad 0 \leq i \leq n-1,$$

are *Gauss periods* of type (n,k) over $\mathbb{F}_q$. Gauss periods over finite fields are highly desirable as normal bases since, when they exist, they have low complexity; see Theorem 5.3.23. Normal bases due to Gauss periods of type $(n,1)$, for all q, and of type $(n,2)$, for $q = 2$, characterize the *optimal normal bases* (Theorem 5.3.6) and have complexity $2n-1$. Gauss periods also often have high order, see Remark 5.3.49. For conditions on when Gauss periods of type (n,k) admit normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, see Theorem 5.3.17. In particular, we note that there is no Gauss period of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ which admits a normal basis when 8 divides n.

Table 2.2.8 gives the lowest k for which a *Gauss period* of type (n,k) admits a normal basis of $\mathbb{F}_{2^n}$ pver $\mathbb{F}_2$ for $n \leq 577$. We give a similar table over $\mathbb{F}_3$ in Table 2.2.9. This range was chosen to cover degrees for common implementations of finite field arithmetic. The output of the table is in the format "n,k'' where k is the minimum number admitting a type (n,k) Gauss period over $\mathbb{F}_{q^n}$, where $q = 2,3$.

2,1	3,2	4,1	5,2	6,2	7,4	9,2	10,1	11,2	12,1	13,4	14,2
15,4	17,6	18,1	19,10	20,3	21,10	22,3	23,2	25,4	26,2	27,6	28,1
29,2	30,2	31,10	33,2	34,9	35,2	36,1	37,4	38,6	39,2	41,2	42,5
43,4	44,9	45,4	46,3	47,6	49,4	50,2	51,2	52,1	53,2	54,3	55,12
57,10	58,1	59,12	60,1	61,6	62,6	63,6	65,2	66,1	67,4	68,9	69,2
70,3	71,8	73,4	74,2	75,10	76,3	77,6	78,7	79,4	81,2	82,1	83,2
84,5	85,12	86,2	87,4	89,2	90,2	91,6	92,3	93,4	94,3	95,2	97,4
98,2	99,2	100,1	101,6	102,6	103,6	105,2	106,1	107,6	108,5	109,10	110,6
111,20	113,2	114,5	115,4	116,3	117,8	118,6	119,2	121,6	122,6	123,10	124,3
125,6	126,3	127,4	129,8	130,1	131,2	132,5	133,12	134,2	135,2	137,6	138,1
139,4	140,3	141,8	142,6	143,6	145,10	146,2	147,6	148,1	149,8	150,19	151,6
153,4	154,25	155,2	156,13	157,10	158,2	159,22	161,6	162,1	163,4	164,5	165,4
166,3	167,14	169,4	170,6	171,12	172,1	173,2	174,2	175,4	177,4	178,1	179,2
180,1	181,6	182,3	183,2	185,8	186,2	187,6	188,5	189,2	190,10	191,2	193,4
194,2	195,6	196,1	197,18	198,22	199,4	201,8	202,6	203,12	204,3	205,4	206,3
207,4	209,2	210,1	211,10	212,5	213,4	214,3	215,6	217,6	218,5	219,4	220,3
221,2	222,10	223,12	225,22	226,1	227,24	228,9	229,12	230,2	231,2	233,2	234,5
235,4	236,3	237,10	238,7	239,2	241,6	242,6	243,2	244,3	245,2	246,11	247,6
249,8	250,9	251,2	252,3	253,10	254,2	255,6	257,6	258,5	259,10	260,5	261,2
262,3	263,6	265,4	266,6	267,8	268,1	269,8	270,2	271,6	273,2	274,9	275,14
276,3	277,4	278,2	279,4	281,2	282,6	283,6	284,3	285,10	286,3	287,6	289,12
290,5	291,6	292,1	293,2	294,3	295,16	297,6	298,6	299,2	300,19	301,10	302,3
303,2	305,6	306,2	307,4	308,15	309,2	310,6	311,6	313,6	314,5	315,8	316,1
317,26	318,11	319,4	321,12	322,6	323,2	324,5	325,4	326,2	327,8	329,2	330,2
331,6	332,3	333,24	334,7	335,12	337,10	338,2	339,8	340,3	341,8	342,6	343,4
345,4	346,1	347,6	348,1	349,10	350,2	351,10	353,14	354,2	355,6	356,3	357,10
358,10	359,2	361,30	362,5	363,4	364,3	365,24	366,22	367,6	369,10	370,6	371,2
372,1	373,4	374,3	375,2	377,14	378,1	379,12	380,5	381,8	382,6	383,12	385,6
386,2	387,4	388,1	389,24	390,3	391,6	393,2	394,9	395,6	396,11	397,6	398,2
399,12	401,8	402,5	403,16	404,3	405,4	406,6	407,8	409,4	410,2	411,2	412,3
413,2	414,2	415,28	417,4	418,1	419,2	420,1	421,10	422,11	423,4	425,6	426,2
427,16	428,5	429,2	430,3	431,2	433,4	434,9	435,4	436,13	437,18	438,2	439,10
441,2	442,1	443,2	444,5	445,6	446,6	447,6	449,8	450,13	451,6	452,11	453,2
454,19	455,26	457,30	458,6	459,8	460,1	461,6	462,10	463,12	465,4	466,1	467,6
468,21	469,4	470,2	471,8	473,2	474,5	475,4	476,5	477,46	478,7	479,8	481,6
482,5	483,2	484,3	485,18	486,10	487,4	489,12	490,1	491,2	492,13	493,4	494,3
495,2	497,20	498,9	499,4	500,11	501,10	502,10	503,6	505,10	506,5	507,4	508,1
509,2	510,3	511,6	513,4	514,33	515,2	516,3	517,4	518,14	519,2	521,32	522,1
523,10	524,5	525,8	526,3	527,6	529,24	530,2	531,2	532,3	533,12	534,7	535,4
537,8	538,6	539,12	540,1	541,18	542,3	543,2	545,2	546,1	547,10	548,5	549,14
550,7	551,6	553,4	554,2	555,4	556,1	557,6	558,2	559,4	561,2	562,1	563,14
564,3	565,10	566,3	567,4	569,12	570,5	571,10	572,5	573,4	574,3	575,2	577,4

Table 2.2.8 Lowest type of a Gauss period forming a normal basis for $q = 2$ and $n \leq 577$.

2,2	3,2	4,1	5,2	6,1	7,4	8,2	9,2	10,3	11,2	13,4	14,2
15,2	16,1	17,6	18,1	19,10	20,5	21,2	22,3	23,2	25,4	26,2	27,4
28,1	29,2	30,1	31,10	32,8	33,6	34,3	35,2	37,4	38,15	39,2	40,7
41,2	42,1	43,4	44,2	45,4	46,3	47,6	49,4	50,2	51,8	52,1	53,2
54,3	55,6	56,2	57,4	58,4	59,12	61,6	62,21	63,2	64,4	65,2	66,3
67,4	68,2	69,2	70,3	71,8	73,4	74,2	75,8	76,10	77,6	78,1	79,4
80,5	81,2	82,9	83,2	85,16	86,2	87,4	88,1	89,2	90,7	91,10	92,5
93,4	94,3	95,2	97,4	98,2	99,2	100,1	101,6	102,11	103,6	104,5	105,2
106,10	107,6	109,10	110,3	111,2	112,1	113,2	114,5	115,4	116,2	117,8	118,9
119,2	121,6	122,3	123,6	124,13	125,2	126,1	127,4	128,2	129,8	130,4	131,2
133,16	134,2	135,4	136,1	137,6	138,1	139,4	140,2	141,2	142,4	143,6	145,10
146,2	147,10	148,1	149,8	150,5	151,6	152,5	153,14	154,3	155,2	157,10	158,2
159,34	160,4	161,6	162,1	163,4	164,5	165,2	166,3	167,14	169,4	170,8	171,12
172,1	173,2	174,9	175,4	176,2	177,4	178,15	179,2	181,6	182,14	183,4	184,7
185,8	186,15	187,6	188,5	189,2	190,3	191,2	193,4	194,2	195,10	196,1	197,18
198,1	199,4	200,2	201,10	202,3	203,12	205,4	206,3	207,4	208,10	209,2	210,1
211,10	212,5	213,6	214,3	215,6	217,6	218,15	219,4	220,4	221,2	222,1	223,12
224,2	225,8	226,15	227,24	229,12	230,2	231,2	232,1	233,2	234,5	235,4	236,8
237,6	238,4	239,2	241,6	242,3	243,2	244,4	245,24	246,3	247,6	248,11	249,8
250,3	251,2	253,4	254,2	255,12	256,1	257,6	258,5	259,10	260,2	261,6	262,3
263,6	265,4	266,8	267,4	268,1	269,8	270,3	271,6	272,5	273,10	274,3	275,12
277,4	278,2	279,10	280,1	281,2	282,1	283,6	284,2	285,2	286,3	287,6	289,12
290,20	291,6	292,1	293,2	294,5	295,12	296,2	297,8	298,4	299,2	301,10	302,3
303,2	304,4	305,6	306,7	307,4	308,2	309,4	310,15	311,6	313,6	314,14	315,2
316,1	317,26	318,17	319,4	320,2	321,18	322,3	323,2	325,4	326,2	327,10	328,7
329,2	330,1	331,6	332,8	333,6	334,15	335,6	337,10	338,2	339,10	340,4	341,8
342,13	343,4	344,5	345,2	346,3	347,6	349,10	350,2	351,22	352,1	353,14	354,3
355,12	356,11	357,4	358,4	359,2	361,30	362,3	363,4	364,7	365,18	366,5	367,6
368,11	369,2	370,4	371,2	373,4	374,3	375,2	376,7	377,14	378,1	379,12	380,5
381,20	382,10	383,12	385,6	386,2	387,14	388,1	389,24	390,5	391,6	392,8	393,10
394,9	395,6	397,6	398,2	399,12	400,1	401,8	402,5	403,4	404,2	405,2	406,21
407,8	409,4	410,2	411,2	412,19	413,2	414,9	415,30	416,5	417,6	418,15	419,2
421,10	422,21	423,4	424,4	425,12	426,3	427,4	428,2	429,2	430,3	431,2	433,4
434,3	435,4	436,13	437,18	438,9	439,10	440,2	441,6	442,3	443,2	445,6	446,15
447,4	448,1	449,8	450,33	451,6	452,8	453,2	454,28	455,2	457,30	458,15	459,8
460,1	461,6	462,1	463,12	464,2	465,10	466,3	467,6	469,10	470,2	471,8	472,4
473,2	474,3	475,4	476,2	477,14	478,4	479,8	481,28	482,3	483,10	484,7	485,2
486,1	487,4	488,2	489,12	490,15	491,2	493,4	494,3	495,30	496,13	497,14	498,11
499,4	500,8	501,16	502,9	503,6	505,10	506,2	507,18	508,1	509,2	510,7	511,6
512,23	513,4	514,3	515,2	517,4	518,9	519,2	520,1	521,32	522,3	523,10	524,2
525,20	526,3	527,6	529,24	530,2	531,2	532,4	533,12	534,27	535,4	536,8	537,8
538,4	539,12	541,18	542,3	543,2	544,10	545,6	546,5	547,10	548,2	549,18	550,21
551,2	553,4	554,2	555,6	556,1	557,6	558,5	559,4	560,5	561,2	562,9	563,14
565,6	566,3	567,28	568,1	569,12	570,1	571,10	572,5	573,4	574,3	575,2	577,4

Table 2.2.9 Lowest type of a Gauss period forming a normal basis for $q = 3$ and $n \leq 577$.

2.2.2.3 Minimum-known complexity of a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, $n \geq 40$

2.2.19 Remark Table 2.2.10 gives the minimum complexity of a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ for $40 \leq n \leq 721$ by using a combination of the exhaustive search data of Table 2.2.4 and theorems from Section 5.3. In each row, we give the degree n, the minimum complexity C_n of a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, the method by which the normal basis was obtained and what property or parameters were used. In the "Method" column, "Optimal" indicates existence of an optimal normal basis, "GNB" indicates the basis arises as a Gauss period and their type is given in the "Property" column. Proposition 5.3.38 constructs normal bases of $\mathbb{F}_{q^n}$ using normal bases of subfields of coprime degree. When this method wins, the values of these coprime factors are indicated in the "Property" column. Corollary 5.3.15 requires an optimal normal basis of $\mathbb{F}_{2^{kn}}$ and the type of the optimal normal basis and the value of k are indicated in the "Property" column. Finally, "sd" indicates that the basis is self-dual.

When n is a power of 2, the best result, when available, is by random search since known methods do not apply. Gauss periods cannot form normal bases when 8 divides n, see Proposition 5.3.20, and n contains no coprime factors with which to apply Proposition 5.3.38. By Conjecture 2.2.15, the complexity of these bases is likely to approach $n^2/2$.

2.2.20 Problem Find constructions of low complexity normal bases of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ when n is a prime power, specifically a power of 2.

n	C_n	Method	Property
40	189	Prop. 5.3.38	$5, 8$
41	81	Optimal	Type 2, sd
42	135	Prop. 5.3.38	$3, 14$
43	165	GNB	$k = 4$, sd
44	147	Prop. 5.3.38	$4, 11$
45	153	Search	[130], sd
46	135	Prop. 5.3.38	$2, 23$
47	261	GNB	$k = 6$, sd
48	425	Prop. 5.3.38	$3, 16$
49	189	GNB	$k = 4$, sd
50	99	Optimal	Type 2, sd
51	101	Optimal	Type 2, sd
52	103	Optimal	Type 1
53	105	Optimal	Type 2, sd
54	209	GNB	$k = 3$
55	189	Prop. 5.3.38	$5, 11$
56	399	Prop. 5.3.38	$7, 8$
57	497	Search	[1263], sd
58	115	Optimal	Type 1
59	597	Search	[1263], sd
60	119	Optimal	Type 1
61	345	GNB	$k = 6$, sd
62	351	GNB	$k = 6$, sd
63	323	Prop. 5.3.38	$7, 9$
64	1829	Random	
65	129	Optimal	Type 2, sd
66	131	Optimal	Type 1
67	261	GNB	$k = 4$, sd
68	567	Prop. 5.3.38	$4, 17$
69	137	Optimal	Type 2, sd
70	207	Prop. 5.3.38	$2, 35$
71	567	GNB	$k = 8$, sd
72	357	Prop. 5.3.38	$8, 9$
73	285	GNB	$k = 4$, sd
74	147	Optimal	Type 2, sd
75	465	Prop. 5.3.38	$3, 25$
76	297	GNB	$k = 3$
77	399	Prop. 5.3.38	$7, 11$
78	231	Prop. 5.3.38	$2, 39$
79	309	GNB	$k = 4$, sd
80	765	Prop. 5.3.38	$5, 16$
81	161	Optimal	Type 2, sd
82	163	Optimal	Type 1
83	165	Optimal	Type 2, sd
84	275	Prop. 5.3.38	$3, 28$
85	729	Prop. 5.3.38	$5, 17$
86	171	Optimal	Type 2, sd
87	285	Prop. 5.3.38	$3, 29$
88	441	Prop. 5.3.38	$8, 11$
89	177	Optimal	Type 2, sd
90	179	Optimal	Type 2, sd
91	525	GNB	$k = 6$, sd
92	315	Prop. 5.3.38	$4, 23$
93	365	GNB	$k = 4$, sd
94	369	GNB	$k = 3$
95	189	Optimal	Type 2, sd
96	1805	Prop. 5.3.38	$3, 32$
97	381	GNB	$k = 4$, sd
98	195	Optimal	Type 2, sd
99	197	Optimal	Type 2, sd
100	199	Optimal	Type 1
101	585	GNB	$k = 6$, sd
102	303	Prop. 5.3.38	$2, 51$
103	597	GNB	$k = 6$, sd
104	945	Prop. 5.3.38	$8, 13$
105	209	Optimal	Type 2, sd
106	211	Optimal	Type 1
107	621	GNB	$k = 6$, sd
108	627	GNB	$k = 5$
109	1081	Cor. 5.3.15	Type 2, $k = 5$, sd
110	399	Prop. 5.3.38	$10, 11$
111	705	Prop. 5.3.38	$3, 37$
112	1615	Prop. 5.3.38	$7, 16$
113	225	Optimal	Type 2, sd
114	663	GNB	$k = 5$
115	405	Prop. 5.3.38	$5, 23$
116	399	Prop. 5.3.38	$4, 29$
117	765	Prop. 5.3.38	$9, 13$
118	687	GNB	$k = 6$, sd
119	237	Optimal	Type 2, sd
120	945	Prop. 5.3.38	$3, 40$
121	705	GNB	$k = 6$, sd
122	711	GNB	$k = 6$, sd
123	405	Prop. 5.3.38	$3, 41$
124	489	GNB	$k = 3$
125	729	GNB	$k = 6$, sd
126	459	Prop. 5.3.38	$9, 14$
127	501	GNB	$k = 4$, sd
128	7821	Random	
129	825	Prop. 5.3.38	$3, 43$
130	259	Optimal	Type 1
131	261	Optimal	Type 2, sd
132	455	Prop. 5.3.38	$4, 33$
133	1595	GNB	$k = 12$, sd
134	267	Optimal	Type 2, sd
135	269	Optimal	Type 2, sd
136	1701	Prop. 5.3.38	$8, 17$
137	801	GNB	$k = 6$, sd
138	275	Optimal	Type 1
139	549	GNB	$k = 4$, sd
140	483	Prop. 5.3.38	$4, 35$
141	1127	GNB	$k = 8$, sd
142	831	GNB	$k = 6$, sd
143	837	GNB	$k = 6$, sd
144	1445	Prop. 5.3.38	$9, 16$
145	513	Prop. 5.3.38	$5, 29$
146	291	Optimal	Type 2, sd
147	861	GNB	$k = 6$, sd
148	295	Optimal	Type 1
149	1191	GNB	$k = 8$, sd
150	495	Prop. 5.3.38	$3, 50$
151	885	GNB	$k = 6$, sd
152	2457	Prop. 5.3.38	$8, 19$
153	605	GNB	$k = 4$, sd
154	567	Prop. 5.3.38	$11, 14$
155	309	Optimal	Type 2, sd
156	515	Prop. 5.3.38	$3, 52$
157	1561	Cor. 5.3.15	Type 2, $k = 5$, sd
158	315	Optimal	Type 2, sd
159	525	Prop. 5.3.38	$3, 53$
160	3249	Prop. 5.3.38	$5, 32$
161	855	Prop. 5.3.38	$7, 23$
162	323	Optimal	Type 1
163	645	GNB	$k = 4$, sd
164	567	Prop. 5.3.38	$4, 41$
165	585	Prop. 5.3.38	$5, 33$
166	495	Prop. 5.3.38	$2, 83$
167	2325	Cor. 5.3.15	Type 2, $k = 7$, sd
168	1995	Prop. 5.3.38	$3, 56$
169	669	GNB	$k = 4$, sd
170	999	GNB	$k = 6$, sd
171	1989	Prop. 5.3.38	$9, 19$
172	343	Optimal	Type 1
173	345	Optimal	Type 2, sd
174	347	Optimal	Type 2, sd
175	693	GNB	$k = 4$, sd
176	1785	Prop. 5.3.38	$11, 16$
177	701	GNB	$k = 4$, sd
178	355	Optimal	Type 1
179	357	Optimal	Type 2, sd
180	359	Optimal	Type 1
181	1065	GNB	$k = 6$, sd
182	721	GNB	$k = 3$
183	365	Optimal	Type 2, sd
184	945	Prop. 5.3.38	$8, 23$
185	1269	Prop. 5.3.38	$5, 37$
186	371	Optimal	Type 2, sd
187	1101	GNB	$k = 6$, sd
188	1107	GNB	$k = 5$
189	377	Optimal	Type 2, sd
190	567	Prop. 5.3.38	$2, 95$
191	381	Optimal	Type 2, sd
192	9145	Prop. 5.3.38	$3, 64$
193	765	GNB	$k = 4$, sd
194	387	Optimal	Type 2, sd
195	645	Prop. 5.3.38	$3, 65$
196	391	Optimal	Type 1
197	3529	Cor. 5.3.15	Type 2, $k = 9$, sd
198	591	Prop. 5.3.38	$2, 99$
199	789	GNB	$k = 4$, sd
200	1953	Prop. 5.3.38	$8, 25$
201	1305	Prop. 5.3.38	$3, 67$
202	1191	GNB	$k = 6$, sd
203	1083	Prop. 5.3.38	$7, 29$
204	707	Prop. 5.3.38	$4, 51$
205	729	Prop. 5.3.38	$5, 41$
206	817	GNB	$k = 3$
207	765	Prop. 5.3.38	$9, 23$
208	3825	Prop. 5.3.38	$13, 16$
209	417	Optimal	Type 2, sd
210	419	Optimal	Type 1
211	2101	Cor. 5.3.15	Type 2, $k = 5$, sd
212	735	Prop. 5.3.38	$4, 53$
213	845	GNB	$k = 4$, sd
214	849	GNB	$k = 3$
215	1269	GNB	$k = 6$, sd

n	C_n	Method	Property
216	2961	Prop. 5.3.38	$8, 27$
217	1281	GNB	$k = 6$, sd
218	1287	GNB	$k = 5$
219	869	GNB	$k = 4$, sd
220	873	GNB	$k = 3$
221	441	Optimal	Type 2, sd
222	735	Prop. 5.3.38	$3, 74$
223	2665	Cor. 5.3.15	Type 2, $k = 6$, sd
224	6859	Prop. 5.3.38	$7, 32$
225	1581	Prop. 5.3.38	$9, 25$
226	451	Optimal	Type 1
227	5447	GNB	$k = 24$, sd
228	1485	Prop. 5.3.38	$3, 76$
229	2747	GNB	$k = 12$, sd
230	459	Optimal	Type 2, sd
231	461	Optimal	Type 2, sd
232	1197	Prop. 5.3.38	$8, 29$
233	465	Optimal	Type 2, sd
234	867	Prop. 5.3.38	$9, 26$
235	933	GNB	$k = 4$, sd
236	937	GNB	$k = 3$
237	1545	Prop. 5.3.38	$3, 79$
238	711	Prop. 5.3.38	$2, 119$
239	477	Optimal	Type 2, sd
240	3825	Prop. 5.3.38	$3, 80$
241	1425	GNB	$k = 6$, sd
242	1431	GNB	$k = 6$, sd
243	485	Optimal	Type 2, sd
244	969	GNB	$k = 3$
245	489	Optimal	Type 2, sd
246	815	Prop. 5.3.38	$3, 82$
247	1461	GNB	$k = 6$, sd
248	4977	Prop. 5.3.38	$8, 31$
249	825	Prop. 5.3.38	$3, 83$
250	2187	Prop. 5.3.38	$2, 125$
251	501	Optimal	Type 2, sd
252	935	Prop. 5.3.38	$9, 28$
253	945	Prop. 5.3.38	$11, 23$
254	507	Optimal	Type 2, sd
255	909	Prop. 5.3.38	$5, 51$
256		No data	Prime power
257	1521	GNB	$k = 6$, sd
258	855	Prop. 5.3.38	$3, 86$
259	2581	Cor. 5.3.15	Type 2, $k = 5$, sd
260	903	Prop. 5.3.38	$4, 65$
261	521	Optimal	Type 2, sd
262	783	Prop. 5.3.38	$2, 131$
263	1557	GNB	$k = 6$, sd
264	1365	Prop. 5.3.38	$8, 33$
265	945	Prop. 5.3.38	$5, 53$
266	1575	GNB	$k = 6$, sd
267	885	Prop. 5.3.38	$3, 89$
268	535	Optimal	Type 1
269	2151	GNB	$k = 8$, sd
270	539	Optimal	Type 2, sd
271	1605	GNB	$k = 6$, sd
272	6885	Prop. 5.3.38	$16, 17$
273	545	Optimal	Type 2, sd
274	2403	Prop. 5.3.38	$2, 137$
275	1953	Prop. 5.3.38	$11, 25$
276	959	Prop. 5.3.38	$4, 69$
277	1101	GNB	$k = 4$, sd
278	555	Optimal	Type 2, sd
279	1109	GNB	$k = 4$, sd
280	1449	Prop. 5.3.38	$8, 35$
281	561	Optimal	Type 2, sd
282	1671	GNB	$k = 6$, sd
283	1677	GNB	$k = 6$, sd
284	1129	GNB	$k = 3$
285	945	Prop. 5.3.38	$3, 95$
286	1071	Prop. 5.3.38	$11, 26$
287	1539	Prop. 5.3.38	$7, 41$
288	6137	Prop. 5.3.38	$9, 32$
289	3457	Cor. 5.3.15	Type 2, $k = 6$, sd
290	1035	Prop. 5.3.38	$5, 58$
291	1725	GNB	$k = 6$, sd
292	583	Optimal	Type 1
293	585	Optimal	Type 2, sd
294	975	Prop. 5.3.38	$3, 98$
295	4719	GNB	$k = 16$, sd
296	2961	Prop. 5.3.38	$8, 37$
297	1761	GNB	$k = 6$, sd
298	1767	GNB	$k = 6$, sd
299	597	Optimal	Type 2, sd
300	995	Prop. 5.3.38	$3, 100$
301	3001	Cor. 5.3.15	Type 2, $k = 5$, sd
302	1201	GNB	$k = 3$
303	605	Optimal	Type 2, sd
304	9945	Prop. 5.3.38	$16, 19$
305	1809	GNB	$k = 6$, sd
306	611	Optimal	Type 2, sd
307	1221	GNB	$k = 4$, sd
308	1155	Prop. 5.3.38	$11, 28$
309	617	Optimal	Type 2, sd
310	927	Prop. 5.3.38	$2, 155$
311	1845	GNB	$k = 6$, sd
312	1617	Prop. 5.3.38	$8, 39$
313	1857	GNB	$k = 6$, sd
314	1863	GNB	$k = 5$
315	1173	Prop. 5.3.38	$9, 35$
316	631	Optimal	Type 1
317	8217	Cor. 5.3.15	Type 2, $k = 13$, sd
318	1055	Prop. 5.3.38	$3, 106$
319	1197	Prop. 5.3.38	$11, 29$
320	16461	Prop. 5.3.38	$5, 64$
321	3105	Prop. 5.3.38	$3, 107$
322	1215	Prop. 5.3.38	$14, 23$
323	645	Optimal	Type 2, sd
324	1127	Prop. 5.3.38	$4, 81$
325	1293	GNB	$k = 4$, sd
326	651	Optimal	Type 2, sd
327	2615	GNB	$k = 8$, sd
328	1701	Prop. 5.3.38	$8, 41$
329	657	Optimal	Type 2, sd
330	659	Optimal	Type 2, sd
331	1965	GNB	$k = 6$, sd
332	1155	Prop. 5.3.38	$4, 83$
333	2397	Prop. 5.3.38	$9, 37$
334	2629	GNB	$k = 7$
335	2349	Prop. 5.3.38	$5, 67$
336	8075	Prop. 5.3.38	$3, 112$
337	3361	Cor. 5.3.15	Type 2, $k = 5$, sd
338	675	Optimal	Type 2, sd
339	1125	Prop. 5.3.38	$3, 113$
340	1353	GNB	$k = 3$
341	2727	GNB	$k = 8$, sd
342	2031	GNB	$k = 6$, sd
343	1365	GNB	$k = 4$, sd
344	3465	Prop. 5.3.38	$8, 43$
345	1233	Prop. 5.3.38	$5, 69$
346	691	Optimal	Type 1
347	2061	GNB	$k = 6$, sd
348	695	Optimal	Type 1
349	3481	Cor. 5.3.15	Type 2, $k = 5$, sd
350	699	Optimal	Type 2, sd
351	3501	Cor. 5.3.15	Type 2, $k = 5$, sd
352	7581	Prop. 5.3.38	$11, 32$
353	4929	Cor. 5.3.15	Type 2, $k = 7$, sd
354	707	Optimal	Type 2, sd
355	2109	GNB	$k = 6$, sd
356	1239	Prop. 5.3.38	$4, 89$
357	1185	Prop. 5.3.38	$3, 119$
358	1071	Prop. 5.3.38	$2, 179$
359	717	Optimal	Type 2, sd
360	3213	Prop. 5.3.38	$5, 72$
361	10801	Cor. 5.3.15	Type 2, $k = 15$, sd
362	2151	GNB	$k = 5$
363	1445	GNB	$k = 4$, sd
364	1449	GNB	$k = 3$
365	2565	Prop. 5.3.38	$5, 73$
366	1095	Prop. 5.3.38	$2, 183$
367	2181	GNB	$k = 6$, sd
368	3825	Prop. 5.3.38	$16, 23$
369	1377	Prop. 5.3.38	$9, 41$
370	1323	Prop. 5.3.38	$5, 74$
371	741	Optimal	Type 2, sd
372	743	Optimal	Type 1
373	1485	GNB	$k = 4$, sd
374	1489	GNB	$k = 3$
375	749	Optimal	Type 2, sd
376	5481	Prop. 5.3.38	$8, 47$
377	2565	Prop. 5.3.38	$13, 29$
378	755	Optimal	Type 1
379	4547	GNB	$k = 12$, sd
380	1323	Prop. 5.3.38	$4, 95$
381	2505	Prop. 5.3.38	$3, 127$
382	1143	Prop. 5.3.38	$2, 191$
383	4595	GNB	$k = 12$, sd
384	39105	Prop. 5.3.38	$3, 128$
385	1449	Prop. 5.3.38	$11, 35$
386	771	Optimal	Type 2, sd
387	1541	GNB	$k = 4$, sd
388	775	Optimal	Type 1
389	9335	GNB	$k = 24$, sd
390	1295	Prop. 5.3.38	$3, 130$
391	2325	GNB	$k = 6$, sd

n	C_n	Method	Property
392	3969	Prop. 5.3.38	$8, 49$
393	785	Optimal	Type 2, sd
394	3915	Cor. 5.3.15	Type 1, $k = 9$
395	2349	GNB	$k = 6$, sd
396	1379	Prop. 5.3.38	$4, 99$
397	2361	GNB	$k = 6$, sd
398	795	Optimal	Type 2, sd
399	4777	Cor. 5.3.15	Type 2, $k = 6$, sd
400	7905	Prop. 5.3.38	$16, 25$
401	3207	GNB	$k = 8$, sd
402	1335	Prop. 5.3.38	$3, 134$
403	6447	GNB	$k = 16$, sd
404	1609	GNB	$k = 3$
405	1449	Prop. 5.3.38	$5, 81$
406	1539	Prop. 5.3.38	$14, 29$
407	2961	Prop. 5.3.38	$11, 37$
408	2121	Prop. 5.3.38	$8, 51$
409	1629	GNB	$k = 4$, sd
410	819	Optimal	Type 2, sd
411	821	Optimal	Type 2, sd
412	1641	GNB	$k = 3$
413	825	Optimal	Type 2, sd
414	827	Optimal	Type 2, sd
415	1485	Prop. 5.3.38	$5, 83$
416	16245	Prop. 5.3.38	$13, 32$
417	1661	GNB	$k = 4$, sd
418	835	Optimal	Type 1
419	837	Optimal	Type 2, sd
420	839	Optimal	Type 1
421	4209	GNB	$k = 10$, sd
422	5053	GNB	$k = 11$
423	1685	GNB	$k = 4$, sd
424	2205	Prop. 5.3.38	$8, 53$
425	2529	GNB	$k = 6$, sd
426	851	Optimal	Type 2, sd
427	6555	Prop. 5.3.38	$7, 61$
428	2547	GNB	$k = 5$
429	857	Optimal	Type 2, sd
430	1539	Prop. 5.3.38	$5, 86$
431	861	Optimal	Type 2, sd
432	11985	Prop. 5.3.38	$16, 27$
433	1725	GNB	$k = 4$, sd
434	3843	Prop. 5.3.38	$2, 217$
435	1733	GNB	$k = 4$, sd
436	6091	GNB	$k = 13$
437	5265	Prop. 5.3.38	$19, 23$
438	875	Optimal	Type 2, sd
439	4381	Cor. 5.3.15	Type 2, $k = 5$, sd
440	3969	Prop. 5.3.38	$5, 88$
441	881	Optimal	Type 2, sd
442	883	Optimal	Type 1
443	885	Optimal	Type 2, sd
444	1475	Prop. 5.3.38	$3, 148$
445	1593	Prop. 5.3.38	$5, 89$
446	2655	GNB	$k = 6$, sd
447	2661	GNB	$k = 6$, sd
448	34751	Prop. 5.3.38	$7, 64$
449	3591	GNB	$k = 8$, sd
450	1683	Prop. 5.3.38	$9, 50$
451	1701	Prop. 5.3.38	$11, 41$
452	1575	Prop. 5.3.38	$4, 113$
453	905	Optimal	Type 2, sd
454	9025	Cor. 5.3.15	Type 1, $k = 19$
455	2451	Prop. 5.3.38	$7, 65$
456	10437	Prop. 5.3.38	$8, 57$
457	13681	Cor. 5.3.15	Type 2, $k = 15$, sd
458	2727	GNB	$k = 6$, sd
459	3671	GNB	$k = 8$, sd
460	919	Optimal	Type 1
461	2745	GNB	$k = 6$, sd
462	1383	Prop. 5.3.38	$2, 231$
463	5545	Cor. 5.3.15	Type 2, $k = 6$, sd
464	4845	Prop. 5.3.38	$16, 29$
465	1545	Prop. 5.3.38	$3, 155$
466	931	Optimal	Type 1
467	2781	GNB	$k = 6$, sd
468	1751	Prop. 5.3.38	$9, 52$
469	1869	GNB	$k = 4$, sd
470	939	Optimal	Type 2, sd
471	3767	GNB	$k = 8$, sd
472	12537	Prop. 5.3.38	$8, 59$
473	945	Optimal	Type 2, sd
474	1575	Prop. 5.3.38	$3, 158$
475	1893	GNB	$k = 4$, sd
476	1659	Prop. 5.3.38	$4, 119$
477	1785	Prop. 5.3.38	$9, 53$
478	1431	Prop. 5.3.38	$2, 239$
479	3831	GNB	$k = 8$, sd
480	16245	Prop. 5.3.38	$3, 160$
481	2865	GNB	$k = 6$, sd
482	2871	GNB	$k = 5$
483	965	Optimal	Type 2, sd
484	1929	GNB	$k = 3$
485	3429	Prop. 5.3.38	$5, 97$
486	1455	Prop. 5.3.38	$2, 243$
487	1941	GNB	$k = 4$, sd
488	7245	Prop. 5.3.38	$8, 61$
489	3225	Prop. 5.3.38	$3, 163$
490	979	Optimal	Type 1
491	981	Optimal	Type 2, sd
492	1863	Prop. 5.3.38	$12, 41$
493	1965	GNB	$k = 4$, sd
494	1969	GNB	$k = 3$
495	989	Optimal	Type 2, sd
496	20145	Prop. 5.3.38	$16, 31$
497	9921	Cor. 5.3.15	Type 2, $k = 10$, sd
498	1815	Prop. 5.3.38	$6, 83$
499	1989	GNB	$k = 4$, sd
500	5103	Prop. 5.3.38	$4, 125$
501	5001	Cor. 5.3.15	Type 2, $k = 5$, sd
502	1503	Prop. 5.3.38	$2, 251$
503	2997	GNB	$k = 6$, sd
504	6783	Prop. 5.3.38	$7, 72$
505	5041	Cor. 5.3.15	Type 2, $k = 5$, sd
506	2835	Prop. 5.3.38	$2, 253$
507	2021	GNB	$k = 4$, sd
508	1015	Optimal	Type 1
509	1017	Optimal	Type 2, sd
510	1919	Prop. 5.3.38	$10, 51$
511	3045	GNB	$k = 6$, sd
512		No data	Prime power
513	2045	GNB	$k = 4$, sd
514	4563	Prop. 5.3.38	$2, 257$
515	1029	Optimal	Type 2, sd
516	1715	Prop. 5.3.38	$3, 172$
517	2061	GNB	$k = 4$, sd
518	2793	Prop. 5.3.38	$7, 74$
519	1037	Optimal	Type 2, sd
520	2709	Prop. 5.3.38	$8, 65$
521	16671	GNB	$k = 32$, sd
522	1043	Optimal	Type 1
523	5221	Cor. 5.3.15	Type 2, $k = 5$, sd
524	1827	Prop. 5.3.38	$4, 131$
525	3465	Prop. 5.3.38	$3, 175$
526	2097	GNB	$k = 3$
527	3141	GNB	$k = 6$, sd
528	5525	Prop. 5.3.38	$16, 33$
529	12695	GNB	$k = 24$, sd
530	1059	Optimal	Type 2, sd
531	1061	Optimal	Type 2, sd
532	2121	GNB	$k = 3$
533	3645	Prop. 5.3.38	$13, 41$
534	1775	Prop. 5.3.38	$3, 178$
535	2133	GNB	$k = 4$, sd
536	5481	Prop. 5.3.38	$8, 67$
537	1785	Prop. 5.3.38	$3, 179$
538	3207	GNB	$k = 6$, sd
539	3969	Prop. 5.3.38	$11, 49$
540	1079	Optimal	Type 1
541	9737	GNB	$k = 18$, sd
542	2161	GNB	$k = 3$
543	1085	Optimal	Type 2, sd
544	29241	Prop. 5.3.38	$17, 32$
545	1089	Optimal	Type 2, sd
546	1091	Optimal	Type 1
547	5469	GNB	$k = 10$, sd
548	3267	GNB	$k = 5$
549	5865	Prop. 5.3.38	$9, 61$
550	2079	Prop. 5.3.38	$11, 50$
551	3285	GNB	$k = 6$, sd
552	2877	Prop. 5.3.38	$8, 69$
553	2205	GNB	$k = 4$, sd
554	1107	Optimal	Type 2, sd
555	2213	GNB	$k = 4$, sd
556	1111	Optimal	Type 1
557	3321	GNB	$k = 6$, sd
558	1115	Optimal	Type 2, sd
559	2229	GNB	$k = 4$, sd
560	5865	Prop. 5.3.38	$16, 35$
561	1121	Optimal	Type 2, sd
562	1123	Optimal	Type 1
563	7869	Cor. 5.3.15	Type 2, $k = 7$, sd
564	2249	GNB	$k = 3$
565	2025	Prop. 5.3.38	$5, 113$
566	2257	GNB	$k = 3$
567	2261	GNB	$k = 4$, sd

n	C_n	Method	Property
568	11907	Prop. 5.3.38	8, 71
569	6817	Cor. 5.3.15	Type 2, $k = 6$, sd
570	2079	Prop. 5.3.38	6, 95
571	5709	GNB	$k = 10$, sd
572	2163	Prop. 5.3.38	11, 52
573	1905	Prop. 5.3.38	3, 191
574	2187	Prop. 5.3.38	14, 41
575	1149	Optimal	Type 2, sd
576	31093	Prop. 5.3.38	9, 64
577	2301	GNB	$k = 4$, sd
578	3447	GNB	$k = 6$, sd
579	3825	Prop. 5.3.38	3, 193
580	2313	GNB	$k = 3$
581	3135	Prop. 5.3.38	7, 83
582	1935	Prop. 5.3.38	3, 194
583	2205	Prop. 5.3.38	11, 53
584	5985	Prop. 5.3.38	8, 73
585	1169	Optimal	Type 2, sd
586	1171	Optimal	Type 1
587	8205	Cor. 5.3.15	Type 2, $k = 7$, sd
588	1955	Prop. 5.3.38	3, 196
589	2349	GNB	$k = 4$, sd
590	6183	Prop. 5.3.38	5, 118
591	3525	GNB	$k = 6$, sd
592	11985	Prop. 5.3.38	16, 37
593	1185	Optimal	Type 2, sd
594	4389	Prop. 5.3.38	11, 54
595	2133	Prop. 5.3.38	5, 119
596	2377	GNB	$k = 3$
597	2381	GNB	$k = 4$, sd
598	1791	Prop. 5.3.38	2, 299
599	4791	GNB	$k = 8$, sd
600	9765	Prop. 5.3.38	3, 200
601	3585	GNB	$k = 6$, sd
602	3249	Prop. 5.3.38	7, 86
603	4437	Prop. 5.3.38	9, 67
604	4789	GNB	$k = 7$
605	3609	GNB	$k = 6$, sd
606	1211	Optimal	Type 2, sd
607	3621	GNB	$k = 6$, sd
608	42237	Prop. 5.3.38	19, 32
609	2429	GNB	$k = 4$, sd
610	5427	Prop. 5.3.38	2, 305
611	1221	Optimal	Type 2, sd
612	1223	Optimal	Type 1
613	6121	Cor. 5.3.15	Type 2, $k = 5$, sd
614	1227	Optimal	Type 2, sd
615	1229	Optimal	Type 2, sd
616	8379	Prop. 5.3.38	7, 88
617	4935	GNB	$k = 8$, sd
618	1235	Optimal	Type 1
619	2469	GNB	$k = 4$, sd
620	2163	Prop. 5.3.38	4, 155
621	3705	GNB	$k = 6$, sd
622	2481	GNB	$k = 3$
623	3363	Prop. 5.3.38	7, 89
624	6545	Prop. 5.3.38	16, 39
625	22465	Cor. 5.3.15	Type 2, $k = 18$, sd
626	5571	Prop. 5.3.38	2, 313
627	2085	Prop. 5.3.38	3, 209
628	4981	GNB	$k = 7$
629	1257	Optimal	Type 2, sd
630	2415	Prop. 5.3.38	18, 35
631	6301	Cor. 5.3.15	Type 2, $k = 5$, sd
632	6489	Prop. 5.3.38	8, 79
633	10505	Prop. 5.3.38	3, 211
634	8839	Cor. 5.3.15	Type 1, $k = 13$
635	4509	Prop. 5.3.38	5, 127
636	2415	Prop. 5.3.38	12, 53
637	2541	GNB	$k = 4$, sd
638	1275	Optimal	Type 2, sd
639	1277	Optimal	Type 2, sd
640	70389	Prop. 5.3.38	5, 128
641	1281	Optimal	Type 2, sd
642	3831	GNB	$k = 6$, sd
643	7705	Cor. 5.3.15	Type 2, $k = 6$, sd
644	2475	Prop. 5.3.38	23, 28
645	1289	Optimal	Type 2, sd
646	1935	Prop. 5.3.38	2, 323
647	9045	Cor. 5.3.15	Type 2, $k = 7$, sd
648	3381	Prop. 5.3.38	8, 81
649	6481	Cor. 5.3.15	Type 2, $k = 5$, sd
650	1299	Optimal	Type 2, sd
651	1301	Optimal	Type 2, sd
652	1303	Optimal	Type 1
653	1305	Optimal	Type 2, sd
654	6435	Prop. 5.3.38	3, 218
655	2349	Prop. 5.3.38	5, 131
656	6885	Prop. 5.3.38	16, 41
657	4845	Prop. 5.3.38	9, 73
658	1315	Optimal	Type 1
659	1317	Optimal	Type 2, sd
660	1319	Optimal	Type 1
661	3945	GNB	$k = 6$, sd
662	2641	GNB	$k = 3$
663	2205	Prop. 5.3.38	3, 221
664	3465	Prop. 5.3.38	8, 83
665	3591	Prop. 5.3.38	7, 95
666	2499	Prop. 5.3.38	9, 74
667	2565	Prop. 5.3.38	23, 29
668	7985	Cor. 5.3.15	Type 1, $k = 11$
669	2669	GNB	$k = 4$, sd
670	2403	Prop. 5.3.38	5, 134
671	4005	GNB	$k = 6$, sd
672	34295	Prop. 5.3.38	3, 224
673	2685	GNB	$k = 4$, sd
674	4023	GNB	$k = 5$
675	13113	Prop. 5.3.38	25, 27
676	1351	Optimal	Type 1
677	5415	GNB	$k = 8$, sd
678	2255	Prop. 5.3.38	3, 226
679	6789	GNB	$k = 10$, sd
680	15309	Prop. 5.3.38	5, 136
681	14961	Cor. 5.3.15	Type 2, $k = 11$, sd
682	4071	GNB	$k = 6$, sd
683	1365	Optimal	Type 2, sd
684	2729	GNB	$k = 3$
685	2733	GNB	$k = 4$, sd
686	1371	Optimal	Type 2, sd
687	6869	GNB	$k = 10$, sd
688	14025	Prop. 5.3.38	16, 43
689	4725	Prop. 5.3.38	13, 53
690	1379	Optimal	Type 2, sd
691	6901	Cor. 5.3.15	Type 2, $k = 5$, sd
692	2415	Prop. 5.3.38	4, 173
693	3743	Prop. 5.3.38	7, 99
694	2769	GNB	$k = 3$
695	4941	Prop. 5.3.38	5, 139
696	5985	Prop. 5.3.38	3, 232
697	2781	GNB	$k = 4$, sd
698	4167	GNB	$k = 5$
699	2325	Prop. 5.3.38	3, 233
700	1399	Optimal	Type 1
701	12601	Cor. 5.3.15	Type 2, $k = 9$, sd
702	7191	Prop. 5.3.38	26, 27
703	4197	GNB	$k = 6$, sd
704	38409	Prop. 5.3.38	11, 64
705	4209	GNB	$k = 6$, sd
706	14787	Prop. 5.3.38	2, 353
707	4221	GNB	$k = 6$, sd
708	1415	Optimal	Type 1
709	2829	GNB	$k = 4$, sd
710	2833	GNB	$k = 3$
711	5253	Prop. 5.3.38	9, 79
712	3717	Prop. 5.3.38	8, 89
713	1425	Optimal	Type 2, sd
714	2607	Prop. 5.3.38	6, 119
715	2709	Prop. 5.3.38	11, 65
716	2499	Prop. 5.3.38	4, 179
717	2385	Prop. 5.3.38	3, 239
718	2151	Prop. 5.3.38	2, 359
719	1437	Optimal	Type 2, sd
720	13005	Prop. 5.3.38	5, 144
721	4305	GNB	$k = 6$, sd

Table 2.2.10 Minimum found complexity of a normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, $40 \leq n \leq 721$.

2.2.3 Resources and standards

2.2.21 Remark The *Combinatorial Object Server* (COS) [2507] allows the user to specify a type of combinatorial object with specific parameter values and COS will return a list of the objects having the desired parameters. In many cases, the format of the output can be chosen to be more machine-readable or human-readable. COS does not rely on a list, rather it generates the objects requested on-the-fly; for this reason, the output is restricted to 200 objects. Examples of the objects generated are permutations, subsets and combinations, set and integer partitions, irreducible and primitive polynomials over small finite fields and spanning trees of a graph.

2.2.22 Remark The *Cunningham project* produces a set of tables to factor the numbers $b^n \pm 1$ for $b = 2, 3, 5, 6, 7, 10, 11, 12$ for n as large as possible. The current factorization methods employed are the elliptic curve method, the multiple polynomial quadratic sieve and the number field sieve. For more information on factorization methods, see [2080, Chapter 3]. The Cunningham tables appear in published form [415] and as an electronic resource [2890].

2.2.23 Remark The *Great Internet Mersenne Prime Search* (GIMPS) [2084] is a distributed computing effort dedicated to finding and verifying Mersenne primes (that is, primes of the form $2^p - 1$, where p is also a prime). GIMPS uses a combination of trial factoring using the Sieve of Eratosthenes, followed by the Pollard $P - 1$ method and ending with the Lucas-Lehmer primality test. For more information on primality testing, see [724, Chapter 31], for example. GIMPS provides the *Prime95* software, which automates all factoring and distributed computing processes. The (currently) largest known Mersenne prime is $2^{43112609} - 1$ containing 12978189 decimal digits [2084].

The search for Mersenne primes is of particular interest in searching for primitive trinomials of large degrees. Primitive polynomials of low-weight are useful in cryptographic applications and pseudo-random number generation; see Sections 14.9 and 16.2. If p is a Mersenne prime, then any irreducible polynomial of degree p over $\mathbb{F}_2$ is primitive. Since binomials of degree at least 2 cannot be irreducible over $\mathbb{F}_2$, we consider trinomials $x^p + x^r + 1$, for some $0 \leq r \leq p - 1$. Sieving trinomials for reducibles is possible by Swan's Theorem; see Section 3.3. For more details on the algorithms and methods used in the search for primitive trinomials, see [408]. An implementation of polynomial arithmetic over $\mathbb{F}_2$ which was motivated by the GIMPS project, entitled *gf2x*, is necessarily highly optimized and is preferred in some finite field software implementations; see Table 2.2.11 for more details.

2.2.24 Remark The *On-Line Encyclopedia of Integer Sequences*^{TM} (OEIS$^{\text{TM}}$) [2800] is a constantly-updated, searchable database of integer sequences. Examples of famous sequences in the OEIS$^{\text{TM}}$ are the Catalan numbers (A000108), prime numbers (A000040), and the Fibonnacci numbers (A000045). Users can search by sequence, "word" (for example, "number of irreducible polynomials" yields sequence A001037) or sequence number. Sequences are sorted lexicographically, so the sequence references may have changed since the date of publication.

2.2.25 Remark In Table 2.2.11, we present a number of software packages which are useful for finite field implementations. We distinguish between packages which are open-source and commercial. We refer the reader to the citation, which provides a current (as of the date of publication) Web URL to the most recent build of the software. We note that this is not an exhaustive list of software packages, simply a useful list of packages used or researched by the author.

Open-source software packages for computations in discrete mathematics

Name	Ver.	Description	
Fast Library for Number Theory (FLINT)	2.3	A C library for performing computations in number theory. Routines include fast algorithms, on par with the other most efficient packages listed, for arbitrary precision integers, rational numbers, modular arithmetic, and p-adic numbers. Most libraries also contain vector, polynomial and matrix methods. Multicore support to come in future versions.	[1426]
Groups, Algorithms, Programming (GAP)	4.4.x	A system for computational discrete algebra emphasizing computational group theory. Can do basic computations with arbitrary integers, rationals, finite fields, p-adic numbers, polynomials, rational functions, and more. Contains a coding theory package, combinatorial functions and prime factorization routines. Provides its own programming language, libraries of algebraic algorithms written in the GAP language as well as data libraries of algebraic objects, particularly various types of groups.	[2796]
gf2x	1.0	Library for efficient arithmetic of single-variable polynomials over $\mathbb{F}_2$. Primarily introduces fast-fourier transform (FFT) for large-degree polynomial multiplication.	[399]
The GNU Multiple Precision Arithmetic Library (GMP)	5.0.x	C/C++ library providing fast arbitrary precision arithmetic on integers, rational numbers, and floating point numbers.	[2797]
Macaulay2	1.4	Software system focusing on algebraic geometry and commutative algebra. Contains core algorithms combined with a high-level interpreted language and debugger to support package creation. Uses elements of *PARI*, *NTL*, and others in its routines.	[1355]
Number Theory Library (NTL)	5.5.x	C++ library providing data structures and routines for arbitrary length integer arithmetic, arbitrary precision floating-point arithmetic, and finite field arithmetic. Also contains lattice basis reduction algorithms and basic linear algebra packages. Interfaces with *gf2x* and *GMP* libraries for additional speed-ups.	[2633]
PARI/GP	2.5.x	C library designed for fast computations in number theory including integer factorization and elliptic curve compututations. Also contains useful function for use with matrices, polynomials, power series, and others. GP is a scripting language used by the gp interactive shell, which accesses the PARI functions. A subset of the GP language can be compiled as C code, resulting in a substantial speed-up.	[2801]

Open-source software packages for computations in discrete mathematics

Name	Ver.	Description	
Singular	3.1.x	A computer algebra system focusing on polynomial computations. Specializes on commutative and non-commutative algebra, algebraic geometry, and singularity theory. Provides a C-like programming language, extendable using libraries. Its core algorithms handle Gröbner bases, polynomial factorization, resultants, and root finding. Advanced libraries and third-party software provide further functionality.	[792]
SAGE	5.0	Comprehensive Python-based open-source computer algebra package. Natively contains a finite field implementation as well as wrappers for other useful packages including Flint, GAP, NTL, PARI, and Singular. Interpreted but contains the ability to compile, using Cython, as C code for a drastic improvement in speed.	[2709]

Commercial stand-alone packages containing finite field implementations

Name	Ver.	Description	
Magma	2.18-x	Computational algebra system focusing on algebra, algebraic combinatorics, algebraic geometry and number theory. Language built to closely approximate the user's mode of thought and usual notation. Major algorithms are designed to give comparable performance to specialized programs. Also contains a number of large databases of elliptic curves, linear codes, irreducible polynomials over finite fields, graphs, Cunningham factorizations, and others.	[712]
Maple	16	Comprehensive computer algebra suite, contains a full featured programming language to create scripts or full applications. A "smart" document environment allows embedding equations, visualizations, or components in the document. Can take advantage of parallelism, multi-threading and multi-process programing. Finite field arithmetic natively given by the "GF" package.	[2002]
Mathematica	8	Development platform concetrating on integrating computation into workflows. Finite field computations are performed using the "FiniteFields" package and "GF" class.	[3004]
Matlab	R2012a	Programming environment for algorithm development and data analysis. Contains arithmetic over finite fields $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ for $n \leq 16$ within the "Communications System Toolbox."	[2799]

Table 2.2.11 Software packages useful for finite field implementations.

See Also

§3.2, §3.3, §3.4	For reducibility and irreducibility of low-weight polynomials.
§5.2, §5.3	For normal bases and their complexities.
§11.1	For computational techniques over finite fields.
[1413], [2080]	For patents and standards of elliptic curve cryptography, most of which contain guidelines for finite field implementations.

References Cited: [130, 399, 408, 415, 712, 724, 792, 1263, 1264, 1355, 1413, 1426, 1631, 1777, 1939, 2002, 2015, 2080, 2084, 2180, 2356, 2507, 2573, 2582, 2633, 2709, 2753, 2796, 2797, 2799, 2800, 2801, 2890, 2925, 3004, 3036]

This page intentionally left blank

II

Theoretical Properties

3

Irreducible polynomials

3.1 Counting irreducible polynomials

Joseph L. Yucas, *Southern Illinois University*

3.1.1 Remark In this section we* are concerned with exact formulae for the number of (univariate) irreducible polynomials over finite fields possessing various properties. There is some overlap with Section 3.5 where specifically polynomials with prescribed coefficients are discussed. Formulae and asymptotic expressions for mutivariate polynomials are given in Section 3.6.

3.1.2 Theorem (Theorem 2.1.24). Denote the number of monic irreducible polynomials of degree n over $\mathbb{F}_q$ by $I_q(n)$. Then

$$I_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}.$$

*The author wishes to thank Stephen Cohen for a number of helpful improvements in this section.

3.1.3 Definition For a positive integer n set

$$D_n = \{r : r|q^n - 1 \text{ but } r \text{ does not divide } q^m - 1 \text{ for } m < n\}.$$

3.1.4 Theorem [3048] We have

$$I_q(n) = \frac{1}{n} \sum_{r \in D_n} \phi(r),$$

where ϕ denotes Euler's function.

3.1.1 Prescribed trace or norm

3.1.5 Definition The *trace* of a monic polynomial f of degree n over $\mathbb{F}_q$ is $-a_1$, where a_1 is the *first coefficient* of f, i.e., the coefficient of x^{n-1} in f. The *norm* of a monic polynomial f of degree n over $\mathbb{F}_q$ is $(-1)^n a_n$, where a_n is the *last coefficient* of f, i.e., the constant term in f. The trace and norm of a monic irreducible polynomial are, respectively, the trace and norm of any of its roots in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

3.1.6 Remark In [2508, 3048] (cited below) and sometimes in the literature, the trace of a polynomial f is taken to be the first coefficient a_1 itself.

3.1.7 Theorem [541, 2508] For a non-zero $a \in \mathbb{F}_q$ the number $I_q(n, a)$ of monic irreducible polynomials of degree n over $\mathbb{F}_q$ with trace a is

$$I_q(n, a) = \frac{1}{qn} \sum_{\substack{d|n \\ (d,q)=1}} \mu(d) q^{n/d}.$$

3.1.8 Theorem [3048] Let q be a power of the prime p. Write $n = p^k m$ with m being p-free (i.e., p does not divide m). The number $I_q(n, 0)$ of monic irreducible polynomials of degree n over $\mathbb{F}_q$ with trace 0 is

$$I_q(n, 0) = \frac{1}{qn} \sum_{d|m} \mu(d) q^{n/d} - \frac{\epsilon}{n} \sum_{d|m} \mu(d) q^{n/dp},$$

where $\epsilon = 1$ if $k > 0$ and $\epsilon = 0$ if $k = 0$.

3.1.9 Definition For $r \in D_n$, write $r = d_r m_r$ where $d_r = \left(r, \frac{q^n - 1}{q - 1}\right)$.

3.1.10 Theorem [3048]

1. Let $r \in D_n$ and suppose $a \in \mathbb{F}_q$ has order m_r. Further, let $I_q(n, r, a)$ denote the number of monic irreducible polynomials over $\mathbb{F}_q$ of degree n, order r and (non-zero) norm a. Then
$$I_q(n, r, a) = \frac{\phi(r)}{n\phi(m_r)}.$$
2. Suppose $a \in \mathbb{F}_q^*$ has order m and let $I_q(n, a)$ denote the number of monic irreducible polynomials over $\mathbb{F}_q$ of degree n with (non-zero) norm a. Then
$$I_q(n, a) = \frac{1}{n\phi(m)} \sum_{\substack{r \in D_n \\ m_r = m}} \phi(r).$$

3.1.11 Remark In [541], Carlitz obtained formulae for the number of monic irreducible polynomials over $\mathbb{F}_q$, q odd, with prescribed trace and whose norm is a (non-zero) square or a non-square, respectively. These involve the quadratic character λ on $\mathbb{F}_q$; thus for $0 \neq b \in \mathbb{F}_q$, $\lambda(b) = 1$ or -1 according as b is a square or non-square in $\mathbb{F}_q$, respectively. (See also Remark 3.5.49.)

3.1.12 Theorem [541, 1783] Let $q = p^m$ be an odd prime power. For $a \in \mathbb{F}_q$ denote by $I_q(n, a, h)$, $h = 1, -1$, respectively, the number of monic irreducible polynomials of degree n over $\mathbb{F}_q$ with trace a whose norm is a (non-zero) square or a non-square. Then,

1. if $a = 0$
$$I_q(n, 0, h) = \begin{cases} \frac{1}{2p}(q^{p-1} - q) & \text{for } n = p, \\ \frac{1}{2n}(q^{n-1} - 1) & \text{for } n \neq p; \end{cases}$$
2. if $a \neq 0$
$$I_q(n, a, h) = \begin{cases} \frac{1}{2p}(q^{p-1} + S) & \text{for } n = p, \\ \frac{1}{2n}(q^{n-1} + S - (-1)^h \lambda(na) - 1) & \text{for } n \neq p, \end{cases}$$

where $S = (-1)^h q^{\frac{n-1}{2}} \lambda((-1)^{\frac{n-1}{2}} a)$, and λ is the quadratic character in $\mathbb{F}_q$.

3.1.2 Prescribed coefficients over the binary field

3.1.13 Remark Subsection 3.5.4 contains various formulae for the numbers of irreducible polynomials with some prescribed coefficients in a general finite field $\mathbb{F}_q$. We list here a specialized result over the binary field $\mathbb{F}_2$ not included there.

3.1.14 Definition For $\beta \in \mathbb{F}_{2^n}$ let

$$T_j(\beta) = \sum_{0 \leq i_1 < i_2 < \cdots < i_j \leq n-1} \beta^{2^{i_1}} \beta^{2^{i_2}} \dots \beta^{2^{i_j}};$$

T_j maps $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ and T_1 is the usual trace function. For $n = 2$ and $j = 3$, we define $T_3(\beta) = 0$ for all $\beta \in \mathbb{F}_4$. For an integer r with $1 \leq r \leq n$, define $F(n, t_1, t_2, \dots, t_r)$ to be the number of elements $\beta \in \mathbb{F}_{2^n}$ with $T_j(\beta) = t_j$ for $j = 1, \dots, r$ and let $(I_2(n, t_1, t_2, \dots, t_r) =)$ $I(n, t_1, t_2, \dots, t_r)$ be the number of monic irreducible polynomials $f(x)$ over $\mathbb{F}_2$ of degree n with coefficient of $x^{n-j} = t_j$ for $j = 1, \dots, r$.

3.1.15 Theorem [3049] We have

$$nI(n,0,0,0) = \sum_{d|n,d \text{ odd}} \mu(d) F(n/d,0,0,0) - \sum_{d|n,d \text{ odd}, n/d \text{ even}} \mu(d) 2^{\frac{n}{2d}-1};$$
$$nI(n,0,0,1) = \sum_{d|n,d \text{ odd}} \mu(d) F(n/d,0,0,1);$$
$$nI(n,0,1,0) = \sum_{d|n,d \text{ odd}} \mu(d) F(n/d,0,1,0) - \sum_{d|n,d \text{ odd}, n/d \text{ even}} \mu(d) 2^{\frac{n}{2d}-1};$$
$$nI(n,0,1,1) = \sum_{d|n,d \text{ odd}} \mu(d) F(n/d,0,1,1);$$
$$nI(n,1,0,0) = \sum_{d|n,d \equiv 1} \mu(d) F(n/d,1,0,0) + \sum_{d|n,d \equiv 3} \mu(d) F(n/d,1,1,1);$$
$$nI(n,1,0,1) = \sum_{d|n,d \equiv 1} \mu(d) F(n/d,1,0,1) + \sum_{d|n,d \equiv 3} \mu(d) F(n/d,1,1,0);$$

$$nI(n,1,1,0) = \sum_{d|n,d\equiv 1} \mu(d)F(n/d,1,1,0) + \sum_{d|n,d\equiv 3} \mu(d)F(n/d,1,0,1);$$
$$nI(n,1,1,1) = \sum_{d|n,d\equiv 1} \mu(d)F(n/d,1,1,1) + \sum_{d|n,d\equiv 3} \mu(d)F(n/d,1,0,0).$$

3.1.16 Remark Explicit formulae for $I(n,t_1,t_2,t_3)$ (the number of irreducible polynomials over $\mathbb{F}_2$ whose first three coefficients are prescribed) can be recovered from Theorem 3.1.15 via the next theorem.

3.1.17 Theorem [1076, 3049] For $n \geq 3$, $F(n,t_1,t_2,t_3) = 2^{n-3} + G(n,t_1,t_2,t_3)$, where the values of $G(n,t_1,t_2,t_3)$ are displayed in the following tables.
1. Case $n = 2m+1$ (in the first column m is calculated modulo 12):

m	000	001	010	011	100	101	110	111
0	$-3\cdot 2^{m-2}$	$3\cdot 2^{m-2}$	2^{m-2}	2^{m-2}	0	0	0	0
1 or 5	2^{m-2}	-2^{m-2}	2^{m-2}	-2^{m-2}	-2^{m-2}	-2^{m-2}	$3\cdot 2^{m-2}$	-2^{m-2}
2 or 10	0	2^{m-1}	0	-2^{m-1}	2^{m-1}	-2^{m-1}	-2^{m-1}	2^{m-1}
3	2^{m-2}	-2^{m-2}	2^{m-2}	-2^{m-2}	2^{m-1}	0	2^{m-1}	-2^m
4 or 8	-2^{m-1}	0	-2^{m-1}	2^m	0	0	0	0
6	$3\cdot 2^{m-2}$	-2^{m-2}	$-3\cdot 2^{m-2}$	2^{m-2}	2^{m-1}	-2^{m-1}	-2^{m-1}	2^{m-1}
7 or 11	2^{m-2}	-2^{m-2}	2^{m-2}	-2^{m-2}	-2^{m-2}	$3\cdot 2^{m-2}$	-2^{m-2}	-2^{m-2}
9	2^{m-2}	-2^{m-2}	2^{m-2}	-2^{m-2}	-2^m	2^{m-1}	0	2^{m-1}

2. Case $n = 2m$ with 3 not dividing n (in the first column m is calculated modulo 4):

m	000	001	010	011	100	101	110	111
0	$3\cdot 2^{m-2}$	-2^{m-2}	-2^{m-2}	-2^{m-2}	$3\cdot 2^{m-2}$	-2^{m-2}	-2^{m-2}	-2^{m-2}
1	$-3\cdot 2^{m-2}$	2^{m-2}	2^{m-2}	2^{m-2}	2^{m-2}	2^{m-2}	2^{m-2}	$-3\cdot 2^{m-2}$
2	$-3\cdot 2^{m-2}$	2^{m-2}	2^{m-2}	2^{m-2}	$-3\cdot 2^{m-2}$	2^{m-2}	2^{m-2}	2^{m-2}
3	$3\cdot 2^{m-2}$	-2^{m-2}	-2^{m-2}	-2^{m-2}	-2^{m-2}	-2^{m-2}	-2^{m-2}	$3\cdot 2^{m-2}$

3. Case $n = 2m$ with 3 dividing n (in the first column m is calculated modulo 4):

m	000	001	010	011	100	101	110	111
0	0	2^{m-1}	2^{m-1}	-2^m	0	2^{m-1}	-2^m	2^{m-1}
1	0	-2^{m-1}	-2^{m-1}	2^m	-2^{m-1}	2^m	-2^{m-1}	0
2	0	-2^{m-1}	-2^{m-1}	2^m	0	-2^{m-1}	2^m	-2^{m-1}
3	0	2^{m-1}	2^{m-1}	-2^m	2^{m-1}	-2^m	-2^{m-1}	0

3.1.18 Remark Formulae for $I(n,t_1,t_2)$ and $F(n,t_1,t_2)$ can be obtained by adding appropriate terms from above [565]. For the binary field these will agree with the earlier general expressions of Kuz'min (Theorems 3.5.43 and 3.5.45) from [1815].

3.1.3 Self-reciprocal polynomials

3.1.19 Remark Self-reciprocal polynomials were defined in Remark 2.1.48. For results on these polynomials see [3050]. Any monic self-reciprocal polynomial R of (even) degree $2n$ has the form $x^n f\left(\frac{x^2+1}{x}\right)$, where f is a monic polynomial of degree n in $\mathbb{F}_q[x]$. (We observe that,

if R is irreducible, then necessarily f is irreducible.) Let $SRMI_q(2n)$ denote number of monic irreducible self-reciprocal polynomials of degree $2n$ over $\mathbb{F}_q$.

3.1.20 Theorem [547, 666, 2091, 2200] If q is odd, then

$$SRMI_q(2n) = \frac{1}{2n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d)(q^{n/d} - 1),$$

and, if q is even, then

$$SRMI_q(2n) = \frac{1}{2n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) q^{n/d}.$$

3.1.21 Remark The notion of self-reciprocal polynomial has recently been generalized and Theorem 3.1.20 extended correspondingly [48].

3.1.22 Definition Let $g(x) = a_1x^2 + b_1x + c_1$ and $h(x) = a_2x^2 + b_2x + c_2$ be relatively prime polynomials over $\mathbb{F}_q$ with $\max(\deg f, \deg g) = 2$ (so that a_1 and a_2 are not both zero). Let $I_q(2n, g, h)$ denote the number of irreducible polynomials (not necessarily monic) of degree $2n$ that can be expressed in the form $h(x)^n f\left(\frac{g(x)}{h(x)}\right)$, where f is a monic polynomial (necessarily irreducible) of degree n.

3.1.23 Theorem [48] Suppose $n > 1$ and g, h are polynomials over $\mathbb{F}_q$ as in Definition 3.1.22. Then

$$I_q(2n, g, h) = \begin{cases} 0 & \text{if } q \text{ is even and } b_1 = b_2 = 0, \\ \frac{1}{2n}(q^n - 1) & \text{if } q \text{ is odd and } n = 2^m, \\ \frac{1}{2n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) q^{n/d} & \text{otherwise.} \end{cases}$$

3.1.24 Remark Theorem 3.1.20 is recovered from Theorem 3.1.23 on setting $g(x) = x^2 + 1$, $h(x) = x$ (using $\sum_{d|n} \mu(d) = 0$ whenever $n > 1$).

3.1.4 Compositions of powers

3.1.25 Definition The *radical* of an integer m (> 1) (denoted here by m^*) is the product of the distinct primes dividing m.

3.1.26 Definition For $t > 1$, a *t-polynomial* T over $\mathbb{F}_q$ of degree tn is one that has the form $T(x) = f(x^t)$ for some monic polynomial f of degree n.

3.1.27 Remark If T is irreducible, then f is also irreducible. Further (see Theorem 3.2.5), (i) $t^*|(q^n - 1)$, and (ii) if $4|t$, then $4|(q^n - 1)$. In fact, if (i) holds then n can be expressed as $n = klm$, where k is the order of q (mod t^*), $l^*|t$, and m and t are relatively prime [666].

3.1.28 Theorem [666] Suppose $t > 1$ and that (i) and (ii) of Remark 3.1.27 hold with $n = klm$. Let $TMI_q(tn)$ be the number of monic irreducible t-polynomials of degree tn. Then

$$TMI_q(tn) = \begin{cases} \dfrac{\phi(t)}{tn}(q^n - 1) & \text{for } m = 1, \\ \dfrac{m\phi(t)}{tn} I_{q^{n/m}}(m) & \text{for } m > 1. \end{cases}$$

3.1.29 Remark For $t > 1$, a *t-reciprocal polynomial* T over $\mathbb{F}_q$ of degree $2tn$ is one that is both a t-polynomial and a self-reciprocal polynomial. Thus it has the form $T(x) = x^{tn} f\left(\frac{x^{2t}+1}{x^t}\right)$, where f is a monic polynomial of degree n. If T is irreducible then f is irreducible. Moreover, from [666] we have (i) t is odd and (ii) $t^* | (q^n + 1)$. Also $2n = klm$, where $l^* | 2t$ and m and $2t$ are relatively prime (so that $m|n$).

3.1.30 Theorem [666, 2200] Suppose $t > 1$ and that (i) and (ii) of Remark 3.1.29 hold with $2n = klm$. Let $TSRMI_q(2tn)$ be the number of monic irreducible t-reciprocal polynomials of degree $2tn$. Then

$$TSRMI_q(2tn) = \begin{cases} \dfrac{\phi(t)}{2tn}(q^n + 1) & \text{for } m = 1, \\ \dfrac{m\phi(t)}{2tn} I_{q^{n/m}}(m) & \text{for } m > 1. \end{cases}$$

3.1.5 Translation invariant polynomials

3.1.31 Definition A polynomial f over $\mathbb{F}_q$ is *translation invariant* if $f(x+a) = f(x)$ for all $a \in \mathbb{F}_q$.

3.1.32 Theorem [2200] Let $TIMI_q(qn)$ denote the number of translation invariant monic irreducible polynomials of degree qn over $\mathbb{F}_q$. Then

$$TIMI_q(qn) = \frac{q-1}{qn} \sum_{\substack{d|n \\ (q,d)=1}} \mu(d) q^{n/d}.$$

3.1.6 Normal replicators

3.1.33 Remark Many of the above formulae and other similar ones can be obtained using the general counting technique [2200] which follows.

3.1.34 Definition A rational function $r = f/g \in \mathbb{F}_q(x)$ is a *replicator* over $\mathbb{F}_q$ if for every $n \geq 1$, $x^{q^n-1} - 1$ divides $f(x)^{q^n} - f(x)g(x)^{q^n-1}$. In this case, we write

$$f(x)^{q^n} - f(x)g(x)^{q^n-1} = (x^{q^n-1} - 1)\widehat{r}(n, x)$$

for some polynomial $\widehat{r}(n, x) \in \mathbb{F}_q[x]$. The polynomial $\widehat{r}(n, x)$ is the *n-th order transform* of r.

3.1.35 Definition Let k be a positive integer. A rational function $r = f/g \in \mathbb{F}_q(x)$ is *k-normal* if for every $n \geq 1$ and for each $\lambda \in \mathbb{F}_{q^n}$, the degrees of the factors of the associated polynomial $f - \lambda g$ divide k, and for some λ, at least one factor has degree equal to k.

3.1.36 Remark For a polynomial $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ over $\mathbb{F}_{q^n}$ we define the following sequence of polynomials:

$$f^{(j)}(x) = x^m + a_{m-1}^{q^j} x^{m-1} + \cdots + a_1^{q^j} x + a_0^{q^j}.$$

We observe that $f^{(s)} = f$ where s is the least common multiple of the degrees of the minimal polynomials of the coefficients of f.

3.1.37 Definition Define the *spin* $S_f(x)$ of the polynomial $f(x)$ by

$$S_f(x) = \prod_{j=0}^{s-1} f^{(j)}(x).$$

3.1.38 Definition Let $r = f/g$ be a k-normal replicator over $\mathbb{F}_q$ and suppose h is an irreducible factor of $f - \lambda g$ for $\lambda \in \mathbb{F}_{q^n}$ of degree d. Then, S_h is *hard* for r if the degree of S_h does not divide n.

3.1.39 Remark Write

$$f^{q^n}(x) - f(x)g^{q^n-1}(x) = (x^{q^n-1} - 1)G(n,x)\bar{r}(n,x),$$

where $\bar{r}(n,x)$ is the factor of $f^{q^n} - fg^{q^n-1}$ of largest degree which is square-free and satisfies $(G(n,x), \bar{r}(n,x)) = 1$. Further let $g(n) = \deg(G(n,x))$. Let $HMI_q(n, r(x))$ denote the number of monic irreducible polynomials of degree n which are hard for r.

3.1.40 Theorem [2200] We have

$$\begin{aligned} HMI_q(kn, r(x)) &= \frac{1}{kn} \sum_{\substack{d|n \\ d \nmid (n/k)}} \mu(n/d)[(m-1)q^n - g(d) + 1] \\ &= \frac{1}{kn} \sum_{\substack{d|n \\ k \nmid d}} \mu(d)[(m-1)q^{n/d} - g(n/d) + 1]. \end{aligned}$$

See Also

§3.5 For further formulae and estimates for irreducible polynomials with prescribed coefficients.
§3.6 For formulae and asymptotic expressions for irreducible multivariate polynomials.

References Cited: [48, 541, 547, 565, 666, 1076, 2091, 2200, 2508, 3048, 3049, 3050]

3.2 Construction of irreducibles

Melsik Kyuregyan, *Armenian National Academy of Sciences*

3.2.1 Construction by composition

3.2.1 Remark Known constructions of irreducible polynomials depend on the composition of an initial irreducible polynomial with a further polynomial or rational function. Often this process can be iterated or continued recursively to produce an infinite sequence of irreducible polynomials of increasing degrees.

3.2.2 Theorem [505, 666] Let f, $g \in \mathbb{F}_q[x]$ be relatively prime polynomials and let $P \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree n. Then the composition

$$F(x) = (g(x))^n \, P\left(f(x)/g(x)\right)$$

is irreducible over $\mathbb{F}_q$ if and only if $f - \alpha g$ is irreducible over $\mathbb{F}_{q^n}$ for any zero $\alpha \in \mathbb{F}_{q^n}$ of P.

3.2.3 Remark Theorem 3.2.2 was employed by several authors [589, 678, 685, 1172, 1820, 1819, 1821, 1822, 1823, 1824, 1939, 2091] to give iterative constructions of irreducible polynomials over finite fields. A further extension of the theorem is produced in [1825], which is also instrumental in the construction of irreducible polynomials of relatively higher degree from given ones.

3.2.4 Theorem [2077] Let $P \in \mathbb{F}_q[x]$ be irreducible of degree n. Then for any $a, b, c, d \in \mathbb{F}_q$ such that $ad - bc \neq 0$,

$$F(x) = (cx + d)^n \, P\left(\frac{ax + b}{cx + d}\right)$$

is also irreducible over $\mathbb{F}_q$.

3.2.5 Theorem [2077] Let t be a positive integer and $P \in \mathbb{F}_q[x]$ be irreducible of degree n and exponent e (equal to the order of any root of P). Then $P(x^t)$ is irreducible over $\mathbb{F}_q$ if and only if

1. $(t, (q^n - 1)/e) = 1$,
2. each prime factor of t divides e, and
3. if $4|t$ then $4|(q^n - 1)$.

3.2.6 Theorem [1939] Let $f_1, f_2, \ldots, f_N$ be all the distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree m and order e, and let $t \geq 2$ be an integer whose prime factors divide e but not $(q^m - 1)/e$. Assume also that $q^m \equiv 1 \pmod 4$ if $t \equiv 0 \pmod 4$. Then $f_1(x^t), f_2(x^t), \ldots, f_N(x^t)$ are all the distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree mt and order et.

3.2.7 Remark Agou [36] has established a criterion for $f(g(x))$ to be irreducible over $\mathbb{F}_q$, where $f, g \in \mathbb{F}_q[x]$ are monic and f is irreducible over $\mathbb{F}_q$. This criterion was used in Agou [36, 38, 39, 40] to characterize irreducible polynomials of special types such as $f\left(x^{p^r} - ax\right)$, $f(x^p - x - b)$, and others. Such irreducible compositions of polynomials are also studied in Cohen [666, 671], Long [1954, 1955], and Ore [2324].

Irreducibility criteria for compositions of polynomials of the form $f(x^t)$ have been established by Agou [34, 35, 36], Butler [469], Cohen [671], Pellet [2376], Petterson [2392], and Serret [2597, 2600]. Berlekamp [231, Chapter 6] and Varshamov and Ananiashvilii [2860] discussed the relationship between the orders of $f(x^t)$ and that of $f(x)$.

3.2.8 Theorem [2077] Let $q = 2^m$ and let $P(x) = \sum_{i=0}^{n} c_i x^i \in \mathbb{F}_q[x]$ be irreducible over $\mathbb{F}_q$ of degree n and $P^*(x) = x^n P\left(\frac{1}{x}\right)$. Denote $\mathbb{F}_{2^m} = F$ and $\mathbb{F}_2 = K$. Then

1. $x^n P\left(x + x^{-1}\right)$ is irreducible over F if and only if $Tr_{F/K}\left(c_1/c_0\right) = 1$;
2. $x^n P^*\left(x + x^{-1}\right)$ is irreducible over F if and only if $Tr_{F/K}\left(c_{n-1}/c_n\right) = 1$.

3.2.9 Remark Part 1 of Theorem 3.2.8 was obtained by Meyn [2091] and by Kyuregyan [1820] in the present general form; for the case $q = 2$ it was earlier obtained by Varshamov and Garakov [2861].

3.2.10 Theorem [2091] Let q be an odd prime power. If P is an irreducible polynomial of degree n over $\mathbb{F}_q$, then $x^n P\left(x + x^{-1}\right)$ is irreducible over $\mathbb{F}_q$ if and only if the element $P(2)P(-2)$ is a non-square in $\mathbb{F}_q$.

3.2.11 Theorem [1822] Let q be odd, $P(x) \neq x$ be an irreducible polynomial of degree $n \geq 1$ over $\mathbb{F}_q$, and $ax^2 + bx + c$ and $dx^2 + rx + h$ be relatively prime polynomials in $\mathbb{F}_q[x]$ with a or d being non-zero and $r^2 \neq 4dh$. Suppose

$$(ah)^2 + (cd)^2 + acr^2 + b^2dh - bcdr - abhr - 2acdh = \delta^2$$

for some $\delta \neq 0$ from $\mathbb{F}_q$. Then the polynomial

$$F(x) = \left(dx^2 + rx + h\right)^n P\left(\frac{ax^2 + bx + c}{dx^2 + rx + h}\right)$$

is irreducible over $\mathbb{F}_q$ if and only if the element

$$\left(r^2 - 4dh\right)^n P\left(\frac{br - 2\left(cd + ah - \delta\right)}{r^2 - 4hd}\right) P\left(\frac{br - 2\left(cd + ah + \delta\right)}{r^2 - 4hd}\right)$$

is a non-square in $\mathbb{F}_q$.

3.2.12 Remark The case $a = c = r = 1$ and $b = d = h = 0$ of Theorem 3.2.11 reduces to Theorem 3.2.10.

3.2.13 Remark We briefly describe some constructive aspects of irreducibility of certain types of polynomials, particularly binomials and trinomials.

3.2.14 Definition A *binomial* is a polynomial with two nonzero terms, one of them being the constant term.

3.2.15 Remark Irreducible binomials can be characterized explicitly. For this purpose it suffices to consider nonlinear, monic binomials.

3.2.16 Theorem [1939] Let $t \geq 2$ be an integer and $a \in \mathbb{F}_q^*$. Then the binomial $x^t - a$ is irreducible in $\mathbb{F}_q[x]$ if and only if the following two conditions are satisfied:

1. each prime factor of t divides the order e of a in $\mathbb{F}_q^*$, but not $(q-1)/e$;
2. $q \equiv 1 \pmod 4$ if $t \equiv 0 \pmod 4$.

3.2.17 Remark Theorem 3.2.16 was essentially shown by Serret [2600] for finite prime fields. Further characterizations of irreducible binomials can be found in Albert [70, Chapter 5], Cappeli [505, 506, 507], Dickson [850, Part I, Chapter 3]. Lowe and Zelinsky [1962], Rédei [2443, Chapter 11], and Schwarz [2568].

3.2.18 Theorem Let a be a nonzero element in an extension field of $\mathbb{F}_q$, $q = 2^A u - 1$, with $A \geq 2$ and u odd. Suppose e is the order of the subgroup of $\mathbb{F}_q^*$ generated by a and the condition

of Part 1 in Theorem 3.2.16 is satisfied for some natural number t divisible by $2^A = 2B$. Then the binomial $x^t - a$ factors as a product of B monic irreducible polynomials in $\mathbb{F}_q[x]$ of degrees $\upsilon = t/B$, that is in $\mathbb{F}_q[x]$ we have the canonical factorization

$$x^t - a = \prod_{j=1}^{B} \left(x^\upsilon - bc_j x^{\upsilon/2} - b^2 \right),$$

where $b = a^r$, $2Br = e/2 + 1 \pmod{(q-1)}$, and the elements $c_1, \ldots, c_B$ are the roots of the polynomial

$$F(x) = \sum_{i=0}^{B/2} \frac{(B-i-1)!B}{i!(B-2i)!} x^{B-2i} \in \mathbb{F}_q[x],$$

and all c_j, $1 \le j \le B$ are in $\mathbb{F}_q$.

3.2.19 Remark The factorization in Theorem 3.2.18 is due to Serret [2600], see also Albert [70, Chapter 5] and Dickson [850, Part I, Chapter 3]. Shiva and Allard [2616] discuss a method for factoring $x^{2^k-1} + 1$ over $\mathbb{F}_2$. The factorization of $x^{q-1} - a$ over $\mathbb{F}_q$ is considered in Dickson [849], see also Agou [37]. Schwarz [2569] has a formula for the number of monic irreducible factors of fixed degree for a given binomial and Rédei [2442] gives a short proof of it; see also Agou [34], Butler [469], and Schwarz [2568]. Gay and Vélez [1261] prove a formula for the degree of the splitting field of an irreducible binomial over an arbitrary field that was shown by Darbi [769] for fields of characteristic 0. Agou [33] studied the factorization of an irreducible binomial over $\mathbb{F}_q$ in an extension field of $\mathbb{F}_q$. Beard and West [213] and McEliece [2046] tabulate factorizations of the binomials $x^n - 1$. The factorization of more general polynomials $g(x)^t - a$ over finite prime fields is considered in Ore [2323] and Petterson [2392]. Applications of factorizations of binomials are contained in Agou [34], Berlekamp [229], and Vaughan [2863].

3.2.20 Definition A *trinomial* is a polynomial with three nonzero terms, one of them being the constant term.

3.2.21 Remark The trinomials that we consider are also affine polynomials.

3.2.22 Theorem [1939] Let $a \in \mathbb{F}_q$ and let p be the characteristic of $\mathbb{F}_q$. Then the trinomial $x^p - x - a$ is irreducible in $\mathbb{F}_q[x]$ if and only if it has no root in $\mathbb{F}_q$.

3.2.23 Corollary [1939] With the notation of Theorem 3.2.22 the trinomial $x^p - x - a$ is irreducible in $\mathbb{F}_q[x]$ if and only if the absolute trace $\mathrm{Tr}_{F/K}(a) \neq 0$, where $F = \mathbb{F}_q$ and $K = \mathbb{F}_p$.

3.2.24 Remark Theorem 3.2.22 and Corollary 3.2.23 were first shown by Pellet [2378]. The fact that $x^p - x - a$ is irreducible over $\mathbb{F}_p$ if $a \in \mathbb{F}_p^*$ was already established by Serret [2597, 2600]. See also Dickson [841], [850, Part I, Chapter 3] and Albert [70, Chapter 5] for these results.

3.2.25 Remark Since for $b \in \mathbb{F}_p^*$ the polynomial $f(x)$ is irreducible over $\mathbb{F}_q$ if and only if $f(bx)$ is irreducible over $\mathbb{F}_q$, the criteria above hold also for trinomials of the form $b^p x^p - bx - a$.

3.2.26 Remark If we consider more general trinomials of the above type for which the degree is a higher power of the characteristic, then these criteria need not be valid any longer. In fact, the following decomposition formula can be established.

3.2.27 Theorem [1939] For $x^q - x - a$ with a being an element of the subfield $K = \mathbb{F}_r$ of $F = \mathbb{F}_q$ we have the decomposition

$$x^q - x - a = \prod_{j=1}^{q/r} (x^r - x - \beta_j)$$

in $\mathbb{F}_q[x]$, where the β_j are the distinct elements of $\mathbb{F}_q$ with $\mathrm{Tr}_{F/K}(\beta_j) = a$.

3.2.28 Remark Theorem 3.2.27 is due to Dickson [841], [850, Part I, Chapter 3], but in the special case $a = 0$ it was already noted by Mathieu [2022].

3.2.29 Theorem [2857, 2858] Let $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be an irreducible polynomial over the finite field $\mathbb{F}_q$ of characteristic p and let $b \in \mathbb{F}_q$. Then the polynomial $P(x^p - x - b)$ is irreducible over $\mathbb{F}_q$ if and only if the absolute trace $\mathrm{Tr}_{F/K}(nb - a_{n-1}) \neq 0$, where $F = \mathbb{F}_q$ and $K = \mathbb{F}_p$.

3.2.30 Remark Theorem 3.2.29 was shown in this general form by Varshamov [2857, 2858]; see also Agou [36]. The case $b = 0$ received considerable attention much earlier. The corresponding result for $b = 0$ and finite prime fields was stated by Pellet [2378] and proved in Pellet [2377]. Polynomials $f(x^p - x)$ over $\mathbb{F}_p$ with $\deg(f)$ a power of p were treated by Serret [2598, 2599]. The case $b = 0$ for arbitrary finite fields was considered in Dickson [850, Part I, Chapter 3] and Albert [70, Chapter 5]. More general types of polynomials such as $f(x^{p^r} - ax)$, $f(x^{p^{2r}} - ax^{p^r} - bx)$ and others have also been studied, see Agou [36, 37, 38, 39, 40, 41, 42], Cohen [671], Long [1953, 1954, 1955, 1956], Long and Vaughan [1957, 1958], and Ore [2324].

3.2.31 Theorem Let $f(x) = x^r - ax - b \in \mathbb{F}_q[x]$, where $r > 2$ is a power of the characteristic of $\mathbb{F}_q$, and suppose that the binomial $x^{r-1} - a$ is irreducible over $\mathbb{F}_q$. Then $f(x)$ is the product of a linear polynomial an an irreducible polynomial over $\mathbb{F}_q$ of degree $r - 1$.

3.2.32 Remark Theorem 3.2.31 generalizes results of Dickson [849] and Albert [70, Chapter 5]. See Schwarz [2571] for further results in this direction.

3.2.2 Recursive constructions

3.2.33 Theorem [1823] Let $q = p^s$ be a prime power and let $f(x) = \sum_{u=0}^{n} c_u x^u$ be a monic irreducible polynomial over $\mathbb{F}_q$. Denote $\mathbb{F}_q = F$ and $\mathbb{F}_p = K$. Suppose that there exists an element $\delta_0 \in \mathbb{F}_q$ such that $f(\delta_0) = a$ with $a \in \mathbb{F}_p^*$, and

$$\mathrm{Tr}_{F/K}(n\delta_0 + c_{n-1}) \cdot \mathrm{Tr}_{F/K}(f'(\delta_0)) \neq 0,$$

where f' is the formal derivative of f. Let $g_0(x) = x^p - x + \delta_0$ and $g_k(x) = x^p - x + \delta_k$, where $\delta_k \in \mathbb{F}_p^*$, $k \geq 1$. Define $f_0(x) = f(g_0(x))$, and $f_k(x) = f_{k-1}^*(g_k(x))$ for $k \geq 1$, where $f_{k-1}^*(x)$ is the monic reciprocal polynomial of $f_{k-1}(x)$, i.e., $f_{k-1}^*(x) = \frac{1}{f_{k-1}(0)} x^{n_{k-1}} f_{k-1}\left(\frac{1}{x}\right)$. Then for each $k \geq 0$ the polynomial $f_k(x)$ is irreducible over $\mathbb{F}_q$ of degree $n_k = n \cdot p^{k+1}$.

3.2.34 Remark The case $s = 1$ and the sequence $(\delta_k)_{k \geq 0}$ is constant, i.e., $\delta_k = \delta \in \mathbb{F}_p^*$ of Theorem 3.2.33, has been studied by Varshamov in [2859], where no proof is given. For a proof see [1172, 2077].

3.2.35 Theorem [1820, 1821, 1823] Let $\delta \in \mathbb{F}_{2^s}^*$ and $f_1(x) = \sum_{u=0}^{n} c_u x^u$ be a monic irreducible polynomial over $\mathbb{F}_{2^s}$ whose coefficients satisfy the conditions

$$Tr_{F/K}\left(\frac{c_1\delta}{c_0}\right) = 1 \text{ and } Tr_{F/K}\left(\frac{c_{n-1}}{\delta}\right) = 1,$$

where $\mathbb{F}_{2^s} = F$ and $\mathbb{F}_2 = K$. Then all the terms in the sequence $(f_k(x))_{k \geq 1}$ defined as

$$f_{k+1}(x) = x^{2^{k-1}n} f_k\left(x + \delta^2 x^{-1}\right), \; k \geq 1,$$

are irreducible polynomials over $\mathbb{F}_{2^s}$.

3.2.36 Theorem [1820, 1821, 2077] Let $f(x) = \sum_{i=0}^{n} c_i x^i$ be irreducible over $\mathbb{F}_{2^m}$ of degree n. Denote $\mathbb{F}_{2^m} = F$ and $\mathbb{F}_2 = K$. Suppose that $\mathrm{Tr}_{F/K}(c_1/c_0) \neq 0$ and $\mathrm{Tr}_{F/K}(c_{n-1}/c_n) \neq 0$. Define the polynomials $a_k(x)$ and $b_k(x)$ recursively by $a_0(x) = x$, $b_0(x) = 1$ and for $k \geq 1$

$$\begin{aligned} a_{k+1}(x) &= a_k(x)b_k(x), \\ b_{k+1}(x) &= a_k^2(x) + b_k^2(x). \end{aligned}$$

Then

$$f_k(x) = (b_k(x))^n \; f\left(a_k(x)/b_k(x)\right)$$

is irreducible over $\mathbb{F}_{2^m}$ of degree $n2^k$ for all $k \geq 0$.

3.2.37 Remark [2077]

1. For the case $q = 2$ in Theorem 3.2.36 the trace function is the identity map on $\mathbb{F}_q$.
2. Let $f(x) = \sum_{i=0}^{n} c_i x^i$ be a monic irreducible polynomial over $\mathbb{F}_2$ of degree n with $c_1 c_{n-1} \neq 0$. Then $f_k(x) = \sum_{i=0}^{n} c_i a_k^i(x) b_k^{n-i}(x)$ is irreducible over $\mathbb{F}_2$ of degree $n2^k$ for all $k \geq 0$.
3. The irreducibility of f_k over $\mathbb{F}_2$ has been studied by several authors, including Varshamov [2859], Wiedemann [2977], Meyn [2091], Gao [1172], Menezes et al. [2077].
4. The irreducibility of f_k over $\mathbb{F}_{2^s}$ has been studied by Kyuregyan [1820, 1819, 1821] and Menezes et al. [1172, 2077].

3.2.38 Theorem [678, 2077] Let f be a monic irreducible polynomial of degree $n \geq 1$ over $\mathbb{F}_q$, q odd, where n is even if $q \equiv 3 \pmod 4$. Suppose that $f(1)f(-1)$ is a non-square in $\mathbb{F}_q$. Define

$$\begin{aligned} f_0(x) &= f(x), \\ f_k(x) &= (2x)^{t_{k-1}} f_{k-1}\left(\left(x + x^{-1}\right)/2\right), \; k \geq 1, \end{aligned}$$

where $t_k = n2^k$ denotes the degree of $f_k(x)$. Then $f_k(x)$ is an irreducible polynomial over $\mathbb{F}_q$ of degree $n2^k$ for every $k \geq 1$.

3.2.39 Remark Further constructions similar to the one from Theorem 3.2.38 can be found in [1822, 1824].

3.2.40 Theorem [1822] Let $P(x) \neq x$ be an irreducible polynomial of degree $n \geq 1$ over $\mathbb{F}_q$, where n is even if $q \equiv 3 \pmod 4$, with $r, h, \delta \in \mathbb{F}_q$ and $r \neq 0$, $\delta \neq 0$. Suppose that $P\left(\frac{2\delta - rh}{r^2}\right) P\left(-\frac{2\delta + rh}{r^2}\right)$ is a non-square in $\mathbb{F}_q$. Define

$$\begin{aligned} F_0(x) &= P(x), \\ F_k(x) &= \left(2x + \frac{2h}{r}\right)^{t_{k-1}} F_{k-1}\left(\left(x^2 + \frac{4\delta^2 - (hr)^2}{r^4}\right) \Big/ \left(2x + \frac{2h}{r}\right)\right), \; k \geq 1, \end{aligned}$$

where $t_k = n2^k$ denotes the degree of $F_k(x)$. Then $F_k(x)$ is an irreducible polynomial over $\mathbb{F}_q$ of degree $n2^k$ for every $k \geq 1$.

3.2.41 Remark For $r = \delta = 2$ and $h = 0$ Theorem 3.2.40 coincides with Theorem 3.2.38 due to Cohen [678, 685]; see also [2077, Theorem 3.24].

3.2.42 Theorem [1822] Let $P(x) \neq x$ be an irreducible polynomial of degree $n \geq 1$ over $\mathbb{F}_q$. Suppose that the elements $P(0), h^n$ and $(2r)^n$ are squares in $\mathbb{F}_q$ and the element $P\left(\frac{2h}{r}\right)$ is

a non-square in $\mathbb{F}_q$. Define

$$\begin{aligned} F_0(x) &= P(x), \\ F_k(x) &= (F_{k-1}(0))^{-1} \left(\frac{(rx+2h)^2}{4h}\right)^{t_{k-1}} F_k\left(\frac{(4h)^2 x}{(rx+2h)^2}\right),\ k \geq 1, \end{aligned}$$

where $t_k = n2^k$ denotes the degree of $F_k(x)$. Then $F_k(x)$ is an irreducible polynomial over $\mathbb{F}_q$ of degree $n2^k$ for every $k \geq 1$.

3.2.43 Theorem [1822] Let P be an irreducible polynomial of degree $n \geq 1$ over $\mathbb{F}_q$, where n is even if $q \equiv 3 \pmod 4$ and $b \in \mathbb{F}_q$. Suppose that the element $P\left(-\frac{b}{2}\right)$ is a non-square in $\mathbb{F}_q$. Define

$$\begin{aligned} F_0(x) &= P(x), \\ F_k(x) &= F_{k-1}\left(x^2 + bx + \frac{b^2}{4} - \frac{b}{2}\right),\ k \geq 1. \end{aligned}$$

Then for every $k \geq 1$, $F_k(x)$ is an irreducible polynomial over $\mathbb{F}_q$ of degree $n2^k$.

3.2.44 Definition For a given polynomial $P(x) = \sum_{u=0}^{n} a_u x^u \in \mathbb{F}_q[x]$ define the polynomial g_P as

$$g_P(x) = (-1)^n \sum_{j=0}^{n} \sum_{u=0}^{2j} (-1)^u a_u a_{2j-u} x^j.$$

3.2.45 Theorem [1824] Let q be an odd prime power and $P(x) = \sum_{u=0}^{n} a_u x^u$ be an irreducible polynomial of degree $n > 1$ over $\mathbb{F}_q$ with at least one coefficient $a_{2i+1} \neq 0$ $\left(0 \leq i \leq \lfloor \frac{n}{2} \rfloor\right)$. Let $ax^2 + 2hx + ahd^{-1}$ and $dx^2 + 2ax + h$ be relatively prime, where $a, d, h, \in \mathbb{F}_q^*$ and $a^2 \neq hd$. Suppose that the element $\left(hd^{-1}\right)^n$ is a non-zero square in $\mathbb{F}_q$ and the element $\left(hd - a^2\right)^n g_{F_0}\left(\frac{h}{d}\right)$ is non-square in $\mathbb{F}_q$ (see Definition 3.2.44 for g_P). Define

$$\begin{aligned} &F_0(x) = P(x), \\ &F_k(x) = H_{k-1}(a,d)^{-1} \left(dx^2 + 2ax + h\right)^{t_{k-1}} F_{k-1}\left(\tfrac{ax^2+2hx+ahd^{-1}}{dx^2+2ax+h}\right), \text{ for } k \geq 1, \end{aligned}$$

where $H_{k-1}(a,d) = d^{t_{k-1}} F_{k-1}\left(\frac{a}{d}\right)$, and t_k is the degree of $F_k(x)$. Then $F_k(x)$ is an irreducible polynomial over $\mathbb{F}_q$ of degree $t_k = n2^k$ for every $k \geq 1$.

3.2.46 Theorem [1824] Let q and P satisfy the hypothesis of Theorem 3.2.45. Suppose $a, c \in \mathbb{F}_q^*$, $(ac)^n$ is a square in $\mathbb{F}_q$ and the element $(-1)^n g_{F_0}\left(\frac{c}{a}\right)$ is a non square in $\mathbb{F}_q$ (see Definition 3.2.44 for g_P). Define

$$\begin{aligned} F_0(x) &= P(x), \\ F_k(x) &= (2x)^{t_{k-1}} F_{k-1}\left(\frac{ax^2 + c}{2ax}\right),\ k \geq 1, \end{aligned}$$

where t_k is the degree of $F_k(x)$. Then $F_k(x)$ is an irreducible polynomial over $\mathbb{F}_q$ of degree $t_k = n2^k$ for every $k \geq 1$.

3.2.47 Remark In particular, the case $q \equiv 3 \pmod 4$) and $F_0(x) = x^2 + 2x + c$ with $a = 1$ of Theorem 3.2.46 was considered by McNay [589]. The case $a = c = 1$ was derived by Cohen; see [678, 685, 2077].

See Also

§3.3 For composite polynomials.
§3.4 For weights of irreducible polynomials.
§3.5 For irreducible polynomials with prescribed coefficients.

References Cited: [33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 70, 213, 229, 231, 469, 505, 506, 507, 589, 666, 671, 678, 685, 769, 841, 849, 850, 1172, 1261, 1819, 1820, 1821, 1822, 1823, 1824, 1825, 1939, 1953, 1954, 1955, 1956, 1957, 1958, 1962, 2022, 2046, 2077, 2091, 2323, 2324, 2376, 2377, 2378, 2392, 2442, 2443, 2568, 2569, 2571, 2597, 2598, 2599, 2600, 2616, 2857, 2858, 2859, 2860, 2861, 2863, 2977]

3.3 Conditions for reducible polynomials

Daniel Panario, *Carleton University*

We present qualitative results on the reducibility of univariate polynomials over finite fields. First we provide some classical work; see the comments at the end of Chapters 3 and 4 of Lidl and Niederreiter [1939] for other results published before 1983. Then we cover several reducibility results that follow from a theorem of Pellet and Stickelberger [2379, 2716].

3.3.1 Composite polynomials

3.3.1 Remark There has been substantial work showing that some classes of polynomials are irreducible using several types of composition of polynomials. Here we are interested in "if and only if" irreducibility statements that as a consequence provide reducibility results.

3.3.2 Remark Let f be a polynomial of degree m over $\mathbb{F}_q$, $q = p^k$, and let L be the linearized polynomial $L(x) = \sum_{i=0}^{n} a_i x^{p^i}$. Ore [2324] considers the irreducibility of $f(L)$. Agou in several articles [37, 39, 41] considers special types of linearized polynomials including $x^{p^r} - ax$ and $x^{p^{2r}} - ax^{p^r} - bx$.

3.3.3 Theorem [37] Let $f(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_0$ be an irreducible polynomial over $\mathbb{F}_q$, $q = p^k$, with root β. Then, for any nonzero a in $\mathbb{F}_q$, $f(x^p - ax)$ is irreducible over $\mathbb{F}_q$ if and only if $a^{(q-1)\gcd(m,p-1)/(p-1)} = 1$ and $\mathrm{Tr}_{km}(\beta/A^p) \neq 0$, where $A \in \mathbb{F}_{q^m}$ satisfies $A^{p-1} = a$ and $\mathrm{Tr}_{km}(x) = x + x^p + \cdots + x^{p^{km-1}}$. In particular, if A is in $\mathbb{F}_q$, then $f(x^p - A^{p-1}x)$ is irreducible over $\mathbb{F}_q$ if and only if $\mathrm{Tr}_k(b_{m-1}/A^p) \neq 0$.

3.3.4 Remark Similar results can be found in the papers by Agou cited above.

3.3.5 Remark We are also interested in results that guarantee classes of polynomials that are reducible. The concluding reducibility result for compositions of the type $f(L)$, where f and L are as above, is given next.

3.3.6 Theorem [41] Let f be an irreducible polynomial of degree m over $\mathbb{F}_q$, $q = p^k$, and let L be the linearized polynomial $L(x) = \sum_{i=0}^{n} a_i x^{p^i}$. If $n \geq 3$, $f(L)$ is reducible.

3.3.7 Remark The cases when $n \leq 2$ in the previous theorem were studied by Agou [39, 40].

3.3.8 Remark Cohen [671, 672] gives alternative proofs for Agou's results.

3.3.9 Remark Moreno [2145] considers the irreducibility of a related composition of functions.

3.3.10 Theorem [2145] Let f and g be polynomials over $\mathbb{F}_q$, $q = p^k$, and let f be irreducible of degree m. The polynomial $f(g(x))$ is irreducible over $\mathbb{F}_q$ if and only if $g(x)+\beta$ is irreducible over $\mathbb{F}_{q^m}$ for any root β of f.

3.3.11 Remark Brawley and Carlitz [394] define root-based polynomial compositions called *composed products*.

3.3.12 Definition Let f and g be monic polynomials in $\mathbb{F}_q^*$ with factorizations in the algebraic closure of $\mathbb{F}_q$, given by

$$f(x) = \prod_{\alpha}(x-\alpha) \quad \text{and} \quad g(x) = \prod_{\beta}(x-\beta).$$

The *composed products* $f \circ g$ and $f \star g$ are defined, respectively, by

$$(f \circ g)(x) = \prod_{\alpha}\prod_{\beta}(x-\alpha\beta), \quad \text{and} \quad (f \star g)(x) = \prod_{\alpha}\prod_{\beta}(x-(\alpha+\beta)).$$

3.3.13 Theorem [394] The composed products of f and g, $f \circ g$ and $f \star g$, are irreducible if and only if f and g are irreducible with coprime degrees.

3.3.14 Remark Related results to composed products can be found in [394, 395, 2103].

3.3.2 Swan-type theorems

3.3.15 Remark Pellet [2379] and Stickelberger [2716] relate the parity of the number of irreducible factors of a squarefree polynomial with its discriminant. When the parity of the number of irreducible factors of a polynomial is even, the polynomial is reducible.

3.3.16 Remark We recall, from Section 2.1, the definition of discriminant (Definition 2.1.135).

3.3.17 Definition Let f be a polynomial of degree n in $\mathbb{F}_q[x]$ with leading coefficient a, and with roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ in its splitting field, counted with multiplicity. The *discriminant* of f is given by

$$D(f) = a^{2n-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2.$$

3.3.18 Remark The discriminant of f is zero if and only if f has multiple roots.

3.3.19 Remark Next is a result given by Stickelberger [2716] although the theorem was originally shown by Pellet [2379]; see also [846].

3.3.20 Theorem [2379, 2716] Let p be an odd prime and suppose that f is a monic polynomial of degree n with integral coefficients in a p-adic field $\mathbb{F}$. Let $\bar{f}$ be the result of reducing the coefficients of f modulo p. Assume further that $\bar{f}$ has no repeated roots. If $\bar{f}$ has r irreducible factors over the residue class field, then $r \equiv n \pmod 2$ if and only if $D(f)$ is a square in $\mathbb{F}$.

3.3.21 Proposition [2753] Let q be a power of an odd prime p and let $\mathbb{F}_q$ be the finite field with q elements. Let g be a polynomial over $\mathbb{F}_q$ of degree n with no repeated roots. Furthermore,

let r be the number of irreducible factors of g over $\mathbb{F}_q$. Then $r \equiv n \pmod 2$ if and only if $D(f)$ is a square in $\mathbb{F}_q$.

3.3.22 Remark Swan extends the previous result to the case $p = 2$ by noting that a p-adic integer a coprime to p, is a p-adic square if and only if a is a square modulo $4p$.

3.3.23 Corollary [2753] Let g be a polynomial of degree n over $\mathbb{F}_2$ with $D(g) \neq 0$ and let f be a monic polynomial over the 2-adic integers such that g is the reduction of f modulo 2. Furthermore, let r be the number of irreducible factors of g over $\mathbb{F}_2$. Then $r \equiv n \pmod 2$ if and only if $D(f) \equiv 1 \pmod 8$.

3.3.24 Remark Swan also characterizes the parity of the number of irreducible factors of a trinomial over $\mathbb{F}_2$. These polynomials are of practical importance when implementing finite field extensions; for example, see [1567] and Section 3.4.

3.3.25 Theorem [2753] Let $n > k > 0$. Assume precisely one of n, k is odd. If r is the number of irreducible factors of $f(x) = x^n + x^k + 1 \in \mathbb{F}_2[x]$, then r is even (and hence f is not irreducible) in the following cases:

1. n even, k odd, $n \neq 2k$ and $nk/2 \equiv 0, 1 \pmod 4$;
2. n odd, k even, $k \nmid 2n$ and $n \equiv 3, 5 \pmod 8$;
3. n odd, k even, $k \mid 2n$ and $n \equiv 1, 7 \pmod 8$.

In other cases f has an odd number of factors.

3.3.26 Remark The case when n and k are both odd can be covered by making use of the fact that the reciprocal polynomial of f has the same number of irreducible factors as f; for reciprocal polynomials see Definition 2.1.48. If both n and k are even the trinomial is a square and has an even number of irreducible factors.

3.3.27 Corollary [2753] Let n be a positive integer divisible by 8. Then every trinomial over $\mathbb{F}_2$ of degree n has an even number of irreducible factors in $\mathbb{F}_2[x]$, and hence it is not irreducible.

3.3.28 Remark Many results have been given following Swan's technique for other types of polynomials and finite field extensions and characteristics. We state several of them starting from characteristic two results and then focusing on odd characteristic.

3.3.29 Remark Vishne [2878] considers trinomials in finite extensions of $\mathbb{F}_2$; see also Theorems 6.69 and 6.695 in [231]. Evaluating the discriminant of a trinomial (modulo $8R$, where R is the valuation ring of the corresponding extension of 2-adic numbers), Vishne's studies are a direct analogue of Swan's proof over $\mathbb{F}_2$.

3.3.30 Corollary [2878] Let $\mathbb{F}_{2^s}$ be an even degree extension of $\mathbb{F}_2$ and n an even number. Then, $g(x) = x^n + ax^k + b \in \mathbb{F}_{2^s}[x]$ has an odd number of irreducible factors only when $g(x) = x^{2d} + ax^d + b$ and $t^2 + at + b$ has no root in $\mathbb{F}_{2^s}$.

3.3.31 Remark Similar results to the one in Corollary 3.3.30 are given in [2878]. Special cases of trinomials of low degrees over extensions of $\mathbb{F}_2$ are given in [570].

3.3.32 Remark Hales and Newhart give a Swan-like result for binary tetranomials; see Theorem 2 in [1399].

3.3.33 Remark It is convenient to use irreducible trinomials over $\mathbb{F}_2$ when constructing extension fields. The usage of pentanomials (polynomials with 5 nonzero coefficients) when trinomials do not exist is in the IEEE standard specifications for public-key cryptography [1567]. However, Scott [2573] shows that some of the recommended irreducible polynomials are not optimal.