

Springer Undergraduate Mathematics Series

S

U

M


S

Arkadii Slinko

Algebra for Applications

Cryptography, Secret Sharing,
Error-Correcting, Fingerprinting,
Compression

Second Edition

 Springer

Springer Undergraduate Mathematics Series

Advisory Editors

M. A. J. Chaplain, St. Andrews, UK

Angus Macintyre, Edinburgh, UK

Simon Scott, London, UK

Nicole Snashall, Leicester, UK

Endre Süli, Oxford, UK

Michael R. Tehranchi, Cambridge, UK

John F. Toland, Bath, UK

The Springer Undergraduate Mathematics Series (SUMS) is a series designed for undergraduates in mathematics and the sciences worldwide. From core foundational material to final year topics, SUMS books take a fresh and modern approach. Textual explanations are supported by a wealth of examples, problems and fully-worked solutions, with particular attention paid to universal areas of difficulty. These practical and concise texts are designed for a one- or two-semester course but the self-study approach makes them ideal for independent use.

More information about this series at <http://www.springer.com/series/3423>

Arkadii Slinko

Algebra for Applications

Cryptography, Secret Sharing,
Error-Correcting, Fingerprinting,
Compression

Second Edition

Arkadii Slinko
Department of Mathematics
The University of Auckland
Auckland, New Zealand

ISSN 1615-2085 ISSN 2197-4144 (electronic)
Springer Undergraduate Mathematics Series
ISBN 978-3-030-44073-2 ISBN 978-3-030-44074-9 (eBook)
<https://doi.org/10.1007/978-3-030-44074-9>

Mathematics Subject Classification (2020): 11A05, 11A07, 11T71, 11Y05, 11Y11, 68P25, 68P30

1st edition: © Springer International Publishing Switzerland 2015

2nd edition: © Springer Nature Switzerland AG 2020

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

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

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

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

*To my parents Michael and Zinaida,
my wife Lilia,
my children Irina and Michael, and
my grandchildren Erik and Yuri.*

Preface to the Second Edition

In our work, we are always between Scylla and Charybdis; we may fail to abstract enough, and miss important physics, or we may abstract too much and end up with fictitious objects in our models turning into real monsters that devour us.

Murray Gell-Mann (*Nobel Prize in Physics in 1969*)

My goals for this edition remain the same. I would like this book to be a basis for a one-semester undergraduate course in applied algebra. I want it to be mathematically rigorous and self-contained, and at the same time to provide a glimpse into the exciting world of applications. The challenge for such a course is to avoid getting overexcited about proving theorems and, on the other hand, not to get bogged down with technical details of the applications. This is a delicate balance, and it is up to the reader to decide how well I managed to steer the exposition between these Scylla and Charybdis.

Apart from correcting misprints and improving the order of exercises I added several small but significant sections that provide links between chapters and make the whole construction of the course more connected. The most notable additions are:

- The chapter on secret sharing (Chap. 6) has now an application to cryptography proper (Chap. 2). By using secret sharing we show how a cryptosystem like RSA can be used by an organisation to share the decryption key between members of that organisation.
- The chapter on polynomials (Chap. 5) was extended by a new section on permutation polynomials which relates this chapter to Chaps. 2 and 3.
- The chapter on compression of information (Chap. 8) was a bit one-sided since it was dealing with encoding of an unknown source but not a known one. The reason was that encoding of an unknown source (universal encoding) has not been adequately reflected in the undergraduate literature while encoding a known source (famous Huffman's codes) was everywhere. However, for the purpose of this book to be self-contained, I wrote a section about Huffman's codes, adding it to Chap. 8.

I also added a number of exercises. Since in the first edition of this book all exercises had solutions (and they still have), I decided to add new exercises (with a few exceptions) without solutions. Those without solutions are marked with a small circle. I also added an index to the book.

Enjoy the book!

Auckland, New Zealand
February 2020

Arkadii Slinko

Preface to the First Edition

The aim of a Lecturer should be, not to gratify his vanity by a shew of originality; but to explain, to arrange, and to digest with clearness, what is already known in the science...

George Pryme (1781–1868)

This book originated from my lecture notes for the one-semester course which I have given many times in The University of Auckland since 1998. The goal of this book is to show the incredible power of algebra and number theory in the real world. It does not advance far in theoretical algebra, theoretical number theory or combinatorics. Instead, we concentrate on concrete objects like groups of points on elliptic curves, polynomial rings and finite fields, study their elementary properties and show their exceptional applicability to various problems in information handling. Among the applications are cryptography, secret sharing, error-correcting, fingerprinting and compression of information.

Some chapters of this book—and especially number-theoretic and cryptographic ones—use GAP for illustrations of the main ideas. GAP is a system for computational discrete algebra, which provides a programming language, a library of thousands of functions implementing algebraic algorithms, written in the GAP language, as well as large data libraries of algebraic objects.

If you are using this book for self-study, then, studying a certain topic, familiarise yourself with the corresponding section of Appendix A, where you will find detailed instructions how to use GAP for this particular topic. As GAP will be useful for most topics, it is not a good idea to skip it completely.

I owe a lot to Robin Christian who in 2006 helped me to introduce GAP to my course and proofread the lecture notes. The introduction of GAP has been the biggest single improvement to this course. The initial version of the GAP notes, which have now been developed into Appendix A, was written by Robin. Stefan Kohl, with the assistance of Eamonn O’Brien, kindly provided us with two programs for GAP that allowed us to calculate in groups of points on elliptic curves. I am grateful to Paul Hafner, Primož Potočnic, Jamie Sneddon and especially to Steven Galbraith who in various years were members of the teaching team for this course and suggested valuable improvements or contributed exercises.

Many thanks go to Shaun White who did a very thorough job proofreading part of the text in 2008 and to Steven Galbraith who improved the section of cryptography in 2009 and commented on the section of compression. However, I bear the sole responsibility for all mistakes and misprints in this book. I would be most obliged if you report any noticed mistakes and misprints to me.

I hope you will enjoy this book as much as I enjoyed writing it.

Auckland
March 2015

Arkadii Slinko

Contents

1	Integers	1
1.1	Natural Numbers	1
1.1.1	Basic Principles	1
1.1.2	Divisibility and Primes	4
1.1.3	Factoring Integers. The Sieve of Eratosthenes	9
1.2	Euclidean Algorithm	14
1.2.1	Divisors and Multiples	14
1.2.2	Greatest Common Divisor and Least Common Multiple	15
1.2.3	Extended Euclidean Algorithm. Chinese Remainder Theorem	18
1.3	Fermat's Little Theorem and Its Generalisations	23
1.3.1	Congruences. Fermat's Little Theorem	23
1.3.2	Euler's ϕ -Function. Euler's Theorem	26
1.4	The Ring of Integers Modulo n . The Field \mathbb{Z}_p	29
1.5	Representation of Numbers	34
2	Cryptology	41
2.1	Classical Secret-Key Cryptology	42
2.1.1	The One-Time Pad	43
2.1.2	An Affine Cryptosystem	46
2.1.3	Hill's Cryptosystem	47
2.2	Modern Public-Key Cryptology	51
2.2.1	One-Way Functions and Trapdoor Functions	52
2.3	Computational Complexity	53
2.3.1	Orders of Magnitude	54
2.3.2	The Time Complexity of Several Number-Theoretic Algorithms	58
2.4	The RSA Public-Key Cryptosystem	62
2.4.1	How Does the RSA System Work?	63
2.4.2	Why Does the RSA System Work?	66
2.4.3	Pseudoprimality Tests	68
2.5	Applications of Cryptology	74

3	Groups	79
3.1	Permutations	79
3.1.1	Composition of Mappings. The Group of Permutations of Degree n	79
3.1.2	Block Permutation Cipher	84
3.1.3	Cycles and Cycle Decomposition	86
3.1.4	Orders of Permutations	88
3.1.5	Analysis of Repeated Actions	91
3.1.6	Transpositions. Even and Odd	93
3.1.7	Puzzle 15	97
3.2	General Groups	100
3.2.1	Definition of a Group. Examples	100
3.2.2	Powers, Multiples and Orders. Cyclic Groups	103
3.2.3	Isomorphism	105
3.2.4	Subgroups	109
3.3	The Abelian Group of an Elliptic Curve	112
3.3.1	Elliptic Curves. The Group of Points of an Elliptic Curve	113
3.3.2	Quadratic Residues and Hasse's Theorem	119
3.3.3	Calculating Large Multiples Efficiently	123
3.4	Applications to Cryptography	124
3.4.1	Encoding Plaintext	124
3.4.2	Additive Diffie–Hellman Key Exchange and the ElGamal Cryptosystem	126
4	Fields	129
4.1	Introduction to Fields	129
4.1.1	Examples and Elementary Properties of Fields	130
4.1.2	Vector Spaces	132
4.1.3	Cardinality of a Finite Field	136
4.2	The Multiplicative Group of a Finite Field is Cyclic	138
4.2.1	Lemmas on Orders of Elements	139
4.2.2	Proof of the Main Theorem	141
4.2.3	Proof of Euler's Criterion	142
4.2.4	Discrete Logarithms	143
4.3	Elgamal Cryptosystem Revisited	144
5	Polynomials	147
5.1	The Ring of Polynomials	147
5.1.1	Introduction to Polynomials	147
5.1.2	Lagrange's Interpolation	152
5.1.3	Factoring Polynomials	154
5.1.4	Greatest Common Divisor and Least Common Multiple	157

5.2	Finite Fields	159
5.2.1	Polynomials Modulo $m(x)$	159
5.2.2	Minimal Annihilating Polynomials	164
5.3	Permutation Polynomials and Applications	167
5.3.1	Permutation Polynomials	167
5.3.2	Cryptosystem Based on a Permutation Polynomial	168
6	Secret Sharing	171
6.1	Introduction to Secret Sharing	172
6.1.1	Access Structure	172
6.1.2	Shamir’s Threshold Access Scheme	173
6.2	A General Theory of Secret Sharing Schemes	176
6.2.1	General Properties of Secret Sharing Schemes	176
6.2.2	Linear Secret Sharing Schemes	181
6.2.3	Ideal and Non-ideal Secret Sharing Schemes	186
6.3	Applications of Secret Sharing	190
7	Error-Correcting Codes	191
7.1	Binary Error-Correcting Codes	192
7.1.1	The Hamming Weight and the Hamming Distance	192
7.1.2	Encoding and Decoding. Simple Examples	195
7.1.3	Minimum Distance, Minimum Weight. Linear Codes	198
7.1.4	Matrix Encoding Technique	202
7.1.5	Parity Check Matrix	207
7.1.6	The Hamming Codes	212
7.1.7	Polynomial Codes	215
7.1.8	Bose–Chaudhuri–Hocquenghem (BCH) Codes	217
7.2	Non-binary Error-Correcting Codes	221
7.2.1	The Basics of Non-binary Codes	221
7.2.2	Reed–Solomon (RS) Codes	224
7.3	Fingerprinting Codes	227
7.3.1	The Basics of Fingerprinting	228
7.3.2	Frameproof Codes	230
7.3.3	Codes with the Identifiable Parent Property	231
8	Compression	235
8.1	Encoding a Known Source	236
8.1.1	Motivating Example	236
8.1.2	Prefix Codes	237
8.1.3	Huffman’s Optimal Code	240
8.2	Encoding an Unknown Source	243
8.2.1	Compressing Binary Sequences (Files)	244
8.2.2	Information and Information Relative to a Partition	245

8.2.3	Fitingof's Compression Code. Encoding	248
8.2.4	Fitingof's Compression Code. Fast Decoding	251
8.3	Information and Uncertainty	254
9	Appendix A: GAP	257
9.1	Computing with GAP	257
9.1.1	Starting with GAP	257
9.1.2	The GAP Interface	257
9.1.3	Programming in GAP: Variables, Lists, Sets and Loops	258
9.2	Number Theory	260
9.2.1	Basic Number-Theoretic Algorithms	260
9.2.2	Arithmetic Modulo m	262
9.2.3	Digitising Messages	264
9.3	Matrix Algebra	266
9.4	Algebra	267
9.4.1	Permutations	267
9.4.2	Elliptic Curves	268
9.4.3	Finite Fields	271
9.4.4	Polynomials	272
10	Appendix B: Miscellanea	275
10.1	Linear Dependency Relationship Algorithm	275
10.2	The Vandermonde Determinant	276
10.3	Stirling's Formula	277
11	Solutions to Exercises	281
11.1	Solutions to Exercises of Chap. 1	281
11.2	Solutions to Exercises of Chap. 2	295
11.3	Solutions to Exercises of Chap. 3	312
11.4	Solutions to Exercises of Chap. 4	326
11.5	Solutions to Exercises of Chap. 5	331
11.6	Solutions to Exercises of Chap. 6	340
11.7	Solutions to Exercises of Chap. 7	346
11.8	Solutions to Exercises of Chap. 8	358
	Literature	363
	Index	365