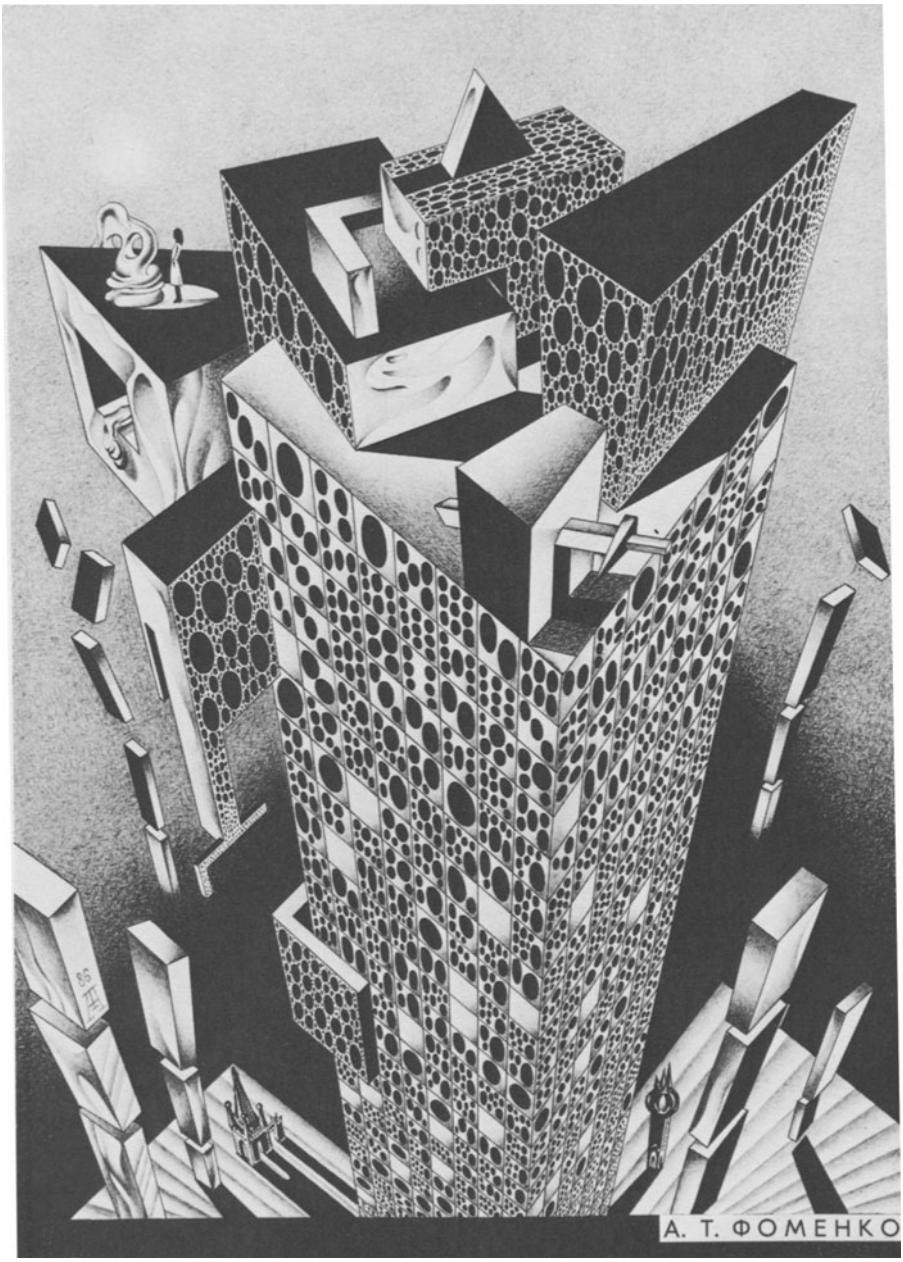
Graduate Texts in Mathematics 114

Springer Science+Business Media, LLC


А. Т. ФОМЕНКО

Neal Koblitz

A Course in Number Theory and Cryptography

Second Edition

Springer

Neal Koblitz
Department of Mathematics
University of Washington
Seattle, WA 98195
USA

Mathematics Subject Classification (2000): 11-01, 11T71

With 5 Illustrations.

Library of Congress Cataloging-in-Publication Data
Koblitz, Neal, 1948–
A Course in number theory and cryptography / Neal Koblitz. — 2nd ed.
p. cm. — (Graduate texts in mathematics ; 114)
Includes bibliographical references and index.
ISBN 978-1-4612-6442-2 ISBN 978-1-4419-8592-7 (eBook)
DOI 10.1007/978-1-4419-8592-7
1. Number theory. 2. Cryptography. I. Title. II. Series.
QA169.M33 1998
512'.7—dc20 94-11613

Printed on acid-free paper.

9 8 7 6 SPIN 11013396

springeronline.com

Foreword

> ...both Gauss and lesser mathematicians may be justified in rejoicing that there is one science [number theory] at any rate, and that their own, whose very remoteness from ordinary human activities should keep it gentle and clean.
>
> — G. H. Hardy, *A Mathematician's Apology*, 1940

G. H. Hardy would have been surprised and probably displeased with the increasing interest in number theory for application to "ordinary human activities" such as information transmission (error-correcting codes) and cryptography (secret codes). Less than a half-century after Hardy wrote the words quoted above, it is no longer inconceivable (though it hasn't happened yet) that the N.S.A. (the agency for U.S. government work on cryptography) will demand prior review and clearance before publication of theoretical research papers on certain types of number theory.

In part it is the dramatic increase in computer power and sophistication that has influenced some of the questions being studied by number theorists, giving rise to a new branch of the subject, called "computational number theory."

This book presumes almost no background in algebra or number theory. Its purpose is to introduce the reader to arithmetic topics, both ancient and very modern, which have been at the center of interest in applications, especially in cryptography. For this reason we take an algorithmic approach, emphasizing estimates of the efficiency of the techniques that arise from the theory. A special feature of our treatment is the inclusion (Chapter VI) of some very recent applications of the theory of elliptic curves. Elliptic curves have for a long time formed a central topic in several branches of theoretical

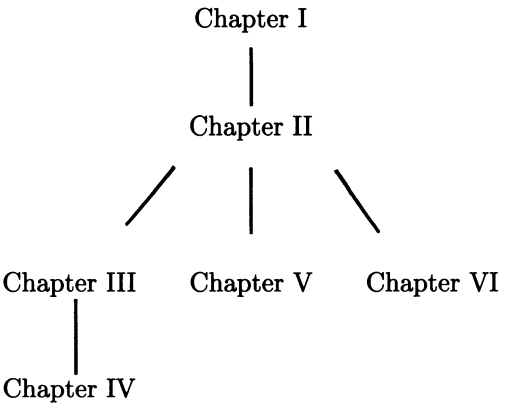
mathematics; now the arithmetic of elliptic curves has turned out to have potential practical applications as well.

Extensive exercises have been included in all of the chapters in order to enable someone who is studying the material outside of a formal course structure to solidify her/his understanding.

The first two chapters provide a general background. A student who has had no previous exposure to algebra (field extensions, finite fields) or elementary number theory (congruences) will find the exposition rather condensed, and should consult more leisurely textbooks for details. On the other hand, someone with more mathematical background would probably want to skim through the first two chapters, perhaps trying some of the less familiar exercises.

Depending on the students' background, it should be possible to cover most of the first five chapters in a semester. Alternately, if the book is used in a sequel to a one-semester course in elementary number theory, then Chapters III–VI would fill out a second–semester course.

The dependence relation of the chapters is as follows (if one overlooks some inessential references to earlier chapters in Chapters V and VI):



This book is based upon courses taught at the University of Washington (Seattle) in 1985–86 and at the Institute of Mathematical Sciences (Madras, India) in 1987. I would like to thank Gary Nelson and Douglas Lind for using the manuscript and making helpful corrections.

The frontispiece was drawn by Professor A. T. Fomenko of Moscow State University to illustrate the theme of the book. Notice that the coded decimal digits along the walls of the building are not random.

This book is dedicated to the memory of the students of Vietnam, Nicaragua and El Salvador who lost their lives in the struggle against U.S. aggression. The author's royalties from sales of the book will be used to buy mathematics and science books for the universities and institutes of those three countries.

Seattle, May 1987

Preface to the Second Edition

As the field of cryptography expands to include new concepts and techniques, the cryptographic applications of number theory have also broadened. In addition to elementary and analytic number theory, increasing use has been made of algebraic number theory (primality testing with Gauss and Jacobi sums, cryptosystems based on quadratic fields, the number field sieve) and arithmetic algebraic geometry (elliptic curve factorization, cryptosystems based on elliptic and hyperelliptic curves, primality tests based on elliptic curves and abelian varieties). Some of the recent applications of number theory to cryptography — most notably, the number field sieve method for factoring large integers, which was developed since the appearance of the first edition — are beyond the scope of this book. However, by slightly increasing the size of the book, we were able to include some new topics that help convey more adequately the diversity of applications of number theory to this exciting multidisciplinary subject.

The following list summarizes the main changes in the second edition.

- Several corrections and clarifications have been made, and many references have been added.
- A new section on zero-knowledge proofs and oblivious transfer has been added to Chapter IV.
- A section on the quadratic sieve factoring method has been added to Chapter V.
- Chapter VI now includes a section on the use of elliptic curves for primality testing.
- Brief discussions of the following concepts have been added: k–threshold schemes, probabilistic encryption, hash functions, the Chor–Rivest knapsack cryptosystem, and the U.S. government's new Digital Signature Standard.

Seattle, May 1994

Contents

Foreword v
Preface to the Second Edition vii

Chapter I. Some Topics in Elementary Number Theory 1
1. Time estimates for doing arithmetic 1
2. Divisibility and the Euclidean algorithm 12
3. Congruences 19
4. Some applications to factoring 27

Chapter II. Finite Fields and Quadratic Residues 31
1. Finite fields 33
2. Quadratic residues and reciprocity 42

Chapter III. Cryptography 54
1. Some simple cryptosystems 54
2. Enciphering matrices 65

Chapter IV. Public Key 83
1. The idea of public key cryptography 83
2. RSA 92
3. Discrete log 97
4. Knapsack 111
5. Zero-knowledge protocols and oblivious transfer 117

Chapter V. Primality and Factoring 125
1. Pseudoprimes 126
2. The rho method 138
3. Fermat factorization and factor bases 143

4. The continued fraction method 154
5. The quadratic sieve method 160

Chapter VI. Elliptic Curves 167
1. Basic facts 167
2. Elliptic curve cryptosystems 177
3. Elliptic curve primality test 187
4. Elliptic curve factorization 191
Answers to Exercises 200
Index 231