Neal Koblitz

A Course in Number Theory and Cryptography

Second Edition

Springer

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

Editorial Board:

S. Axler
Mathematics Department
San Francisco State
University
San Francisco, CA 94132
USA
axler@sfu.edu

F. W. Gehring
Mathematics Department
East Hall
University of Michigan
Ann Arbor, MI 48109
USA
fgehring@math.lsa.umich.edu

K. A. Ribet
Mathematics Department
University of California,
Berkeley
Berkeley, CA 94720-3840
USA
ribet@math.berkeley.edu

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.

© 1994 Springer Science+Business Media New York
Originally published by springer-Verlag New York, Inc. in 1994
Softcover reprint of the hardcover 2nd edition 1994
All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer-Verlag New York, Inc., 175 Fifth Avenue, New York, NY 10010, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.
The use of general descriptive names, trade names, trademarks, etc., in this publication, even if the former are not especially identified, is not to be taken as a sign that such names, as understood by the Trade Marks and Merchandise Marks Act, may accordingly be used freely by anyone.

9 8 7 6 SPIN 11013396

springeronline.com

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