Graduate Texts in Mathematics 114

Editorial Board
J.H. Ewing F.W. Gehring P.R. Halmos

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

Editorial Board

J.H. Ewing	F.W. Gehring	P.R. Halmos
Department of Mathematics	Department of Mathematics	Department of Mathematics
Indiana University	University of Michigan	Santa Clara University
Bloomington, IN 47405	Ann Arbor, MI 48109	Santa Clara, CA 95053
USA	USA	USA

Mathematics Subject Classifications (1991): 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 0-387-94293-9 (New York : acid-free). — ISBN 3-540-94293-9 (Berlin : acid-free)
1. Number theory 2. Cryptography. I. Title. II. Series.
QA241.K672 1994
512'.7—dc20 94-11613

© 1994, 1987 Springer-Verlag New York, Inc.
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.

Production managed by Hal Henglein; manufacturing supervised by Genieve Shaw.
Photocomposed pages prepared from the author's TeX file.
Printed and bound by R.R. Donnelley & Sons, Harrisonburg, VA.
Printed in the United States of America.

9 8 7 6 5 4 3 2 1

ISBN 0-387-94293-9 Springer-Verlag New York Berlin Heidelberg
ISBN 3-540-94293-9 Springer-Verlag Berlin Heidelberg New York