



DIMACS

Series in Discrete Mathematics
and Theoretical Computer Science

Volume 64

Unusual Applications of Number Theory

DIMACS Workshop
Unusual Applications of Number Theory
January 10–14, 2000
DIMACS Center

Melvyn B. Nathanson
Editor



American Mathematical Society

DIMACS

Series in Discrete Mathematics
and Theoretical Computer Science

Volume 64

Unusual Applications of Number Theory

DIMACS Workshop
Unusual Applications of Number Theory
January 10–14, 2000
DIMACS Center

Melvyn B. Nathanson
Editor

Center for Discrete Mathematics
and Theoretical Computer Science
A consortium of Rutgers University, Princeton University,
AT&T Labs–Research, Bell Labs (Lucent Technologies),
NEC Laboratories America, and Telcordia Technologies
(with partners at Avaya Labs, IBM Research, and Microsoft Research)



American Mathematical Society

This DIMACS volume presents the proceedings from the workshop Unusual Applications of Number Theory held at the DIMACS Center, Rutgers University, January 10–14, 2000.

2000 *Mathematics Subject Classification*. Primary 11Z05.

Library of Congress Cataloging-in-Publication Data

DIMACS Workshop on Unusual Applications of Number Theory (2000 : Piscataway, N.J.)

Unusual applications of number theory : DIMACS workshop, unusual applications of number theory, January 10–14, 2000, DIMACS Center / Melvyn B. Nathanson, editor.

p. cm. — (DIMACS series in discrete mathematics and theoretical computer science ; v. 64)
ISBN 0-8218-2703-0 (alk. paper)

1. Number theory—Congresses. I. Nathanson, Melvyn B. (Melvyn Bernard), 1944– II. Title. III. Series.

QA241.D56 2000
512.7—dc22

2004043691

Copying and reprinting. Material in this book may be reproduced by any means for educational and scientific purposes without fee or permission with the exception of reproduction by services that collect fees for delivery of documents and provided that the customary acknowledgment of the source is given. This consent does not extend to other kinds of copying for general distribution, for advertising or promotional purposes, or for resale. Requests for permission for commercial use of material should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, Rhode Island 02904-2294, USA. Requests can also be made by e-mail to reprint-permission@ams.org.

Excluded from these provisions is material in articles for which the author holds copyright. In such cases, requests for permission to use or reprint should be addressed directly to the author(s). (Copyright ownership is indicated in the notice in the lower right-hand corner of the first page of each article.)

© 2004 by the American Mathematical Society. All rights reserved.

The American Mathematical Society retains all rights
except those granted to the United States Government.
Printed in the United States of America.

∞ The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.
Visit the AMS home page at <http://www.ams.org/>

10 9 8 7 6 5 4 3 2 1 09 08 07 06 05 04

Contents

Foreword	v
Preface	vii
A four parameter generalization of Göllnitz's (big) partition theorem K. ALLADI, G. E. ANDREWS, AND A. BERKOVICH	1
The Friedman-Joichi-Stanton monotonicity conjecture at primes GEORGE E. ANDREWS	9
A group theoretic approach to public-key cryptography IRIS ANSHEL, MICHAEL ANSHEL, BENJI FISHER, AND DORIAN GOLDFELD	17
Dedekind sums: a combinatorial-geometric viewpoint MATTHIAS BECK AND SINAI ROBINS	25
Noncommutative number theory PAULA B. COHEN	37
An application of structure theory of set addition to a question in ergodic theory JEAN-MARC DESHOUILERS, GREGORY FREIMAN, AND ALEXANDER A. YUDIN	53
Linear algebra and additive theory J. A. DIAS DA SILVA	61
On the distribution of the power generator modulo a prime power JOHN B. FRIEDLANDER, JAN S. dT. HANSEN, AND IGOR E. SHPARLINSKI	71
Number theoretical error estimates in a quantization scheme for bandlimited signals C. SINAN GÜNTÜRK	81
Random walks with badly approximable numbers DOUG HENSLEY AND FRANCIS EDWARD SU	95
Distribution of values of real quadratic zeta functions JOSHUA HOLDEN	103

Standardizing nonstandard methods for upper Banach density problems RENLING JIN	109
On homogeneous linear recurrence relations and approximation of zeros of complex polynomials BAHMAN KALANTARI	125
Formal power series arising from multiplication of quantum integers MELVYN B. NATHANSON	145
Formal languages and number theory JEFFREY SHALLIT	169
Lattices, cryptography, and the NTRU public key cryptosystem JOSEPH H. SILVERMAN	183
Zeta functions of graph coverings H. M. STARK AND A. A. TERRAS	199
Comparison of Selberg's trace formula with its discrete analogues AUDREY TERRAS	213
Unusual applications of quadratic Gaussian sums CARLOS JULIO MORENO AND AARON WAN	227

Foreword

A workshop on Unusual Applications of Number Theory was held at Rutgers University on January 10-14, 2000. We would like to express our appreciation to George Andrews, David Chudnovsky, Ron Graham, Jeff Lagarias, Victor Miller, Mel Nathanson, Andrew Odlyzko, and Carl Pomerance for their efforts to organize and plan this successful conference.

Number theory is an old and fascinating topic of great interest in and of itself, but one with a remarkably large number of applications in and connections to other areas of research, many of them not so well known. This workshop was centered around applications and interactions of number theory with other areas of science and of mathematics. Topics explored included physics, combinatorics, ergodic theory, spectral theory, geometry, and numerical analysis, as well as the more “standard” topics of computer science and cryptography.

DIMACS gratefully acknowledges the generous support that makes these programs possible. The National Science Foundation and the New Jersey Commission on Science and Technology, DIMACS’ partners at Rutgers, Princeton, AT&T Labs-Research, Bell Labs, NEC Laboratories America, and Telcordia Technologies, and its affiliated partners at Avaya Labs, HP Labs, IBM Research, and Microsoft Research have generously supported the workshop program at DIMACS that makes this type of workshop possible.

Fred S. Roberts
Director

Robert Tarjan
Co-Director for Princeton

This page intentionally left blank

Preface

These are the proceedings of the DIMACS Workshop on Unusual Applications of Number Theory, which was held at the DIMACS Center of Rutgers University in Piscataway, New Jersey, on January 10–14, 2000. The usual applications of number theory are to computer science and cryptology. In this workshop, the organizers looked for other applications of number theory, as well as topics in number theory with potential applications in science and engineering.

The organizing committee of this workshop was Mel Nathanson (Chair), George Andrews, David Chudnovsky, Ron Graham, Jeff Lagarias, Victor Miller, Andrew Odlyzko, and Carl Pomerance. I thank the members of this committee for their help in suggesting and inviting speakers to this meeting.

It was a pleasure to work with DIMACS Director Fred Roberts and his staff on this workshop. I am especially grateful to Mel Janowitz of DIMACS, who provided crucial and efficient editorial assistance with these proceedings, and who made sure that the LaTeX files of the papers in this volume satisfied AMS publication requirements.

Partial support for this conference was provided by the National Science Foundation and the New Jersey Commission on Science and Technology.

Melvyn B. Nathanson
Short Hills, New Jersey
January 16, 2004

This page intentionally left blank

This volume contains the proceedings of the workshop held at the DIMACS Center of Rutgers University (Piscataway, NJ) on Unusual Applications of Number Theory. Standard applications of number theory are to computer science and cryptology. In this volume, well-known number theorist, Melvyn B. Nathanson, gathers articles from the workshop on other, less standard applications in number theory, as well as topics in number theory with potential applications in science and engineering.

The material is suitable for graduate students and researchers interested in number theory and its applications.

ISBN 0-8218-2703-0



9 780821 827031

DIMACS/64

AMS *on the Web*
www.ams.org