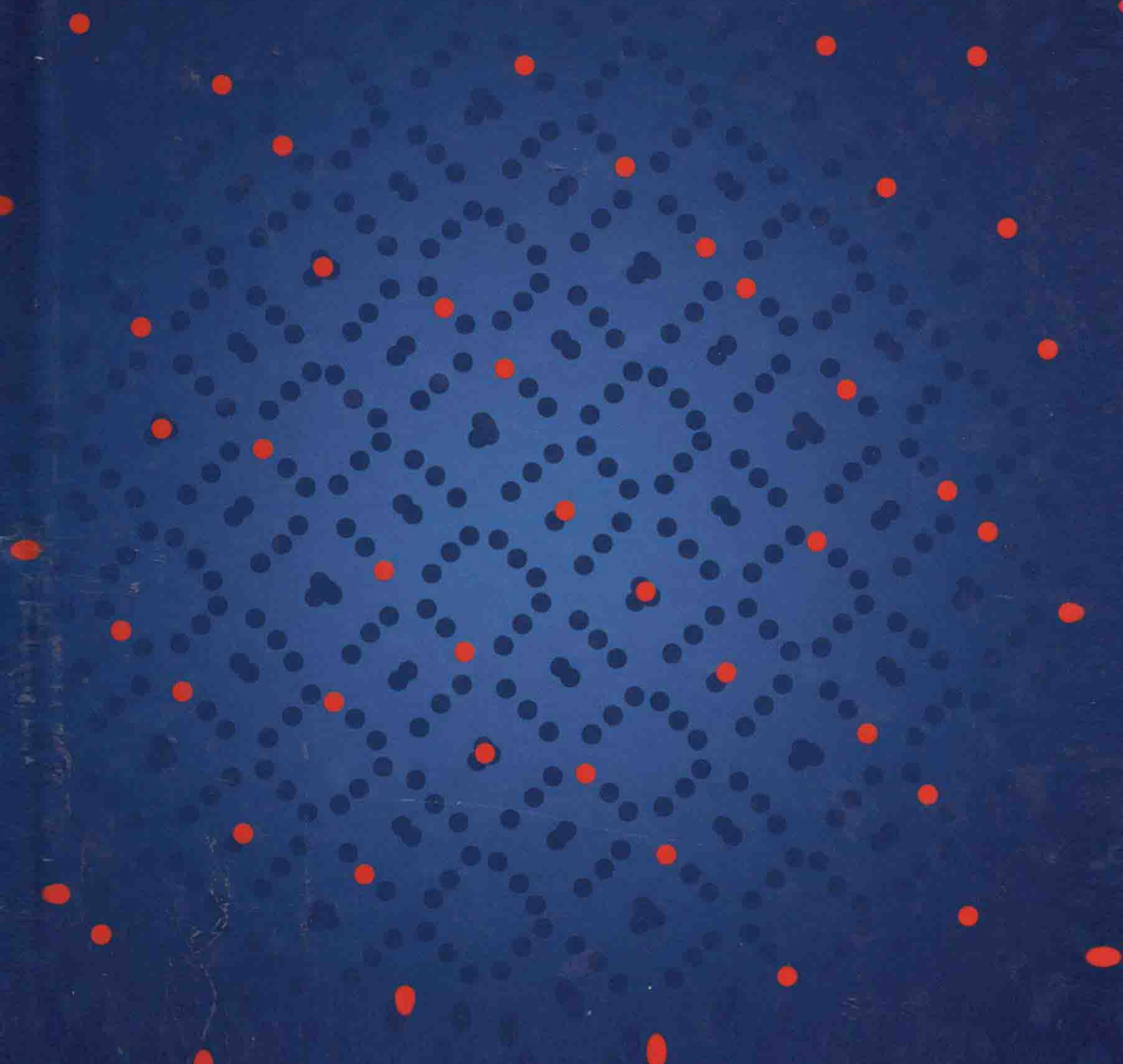
Applied Algebra
a[redacted]mber Theory

DITED BY

Gerhard Larcher, Friedrich Pillichshammer,
Arne Winterhof and Chaoping Xing



Applied Algebra and Number Theory

Essays in Honor of Harald Niederreiter on the occasion of his 70th birthday

Edited by

GERHARD LARCHER
Johannes Kepler University Linz

FRIEDRICH PILLICHSHAMMER
Johannes Kepler University Linz

ARNE WINTERHOF
Austrian Academy of Sciences, Linz

CHAOPING XING
Nanyang Technological University, Singapore

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107074002

First published 2014

Printed in the United Kingdom by Clays, St Ives plc

A catalog record for this publication is available from the British Library

Library of Congress Cataloging in Publication data
Applied Algebra and Number Theory : Essays in Honor of Harald Niederreiter on the occasion of his 70th birthday / edited by Gerhard Larcher, Johannes Kepler Universität Linz, Friedrich Pillichshammer, Johannes Kepler Universität Linz, Arne Winterhof, Austrian Academy of Sciences, Linz, Chaoping Xing, Nanyang Technological University, Singapore.
pages cm
Includes bibliographical references.
ISBN 978-1-107-07400-2 (hardback)
1. Number theory. I. Niederreiter, Harald, 1944- honoree. II. Larcher, Gerhard, editor.
QA241.A67 2014
512.7–dc23
2014013624

ISBN 978-1-107-07400-2 Hardback

Applied Algebra and Number Theory

Essays in Honor of Harald Niederreiter on the occasion of his 70th birthday

Harald Niederreiter's pioneering research in the field of applied algebra and number theory has led to important and substantial breakthroughs in many areas. This collection of survey articles has been authored by close colleagues and leading experts to mark the occasion of his 70th birthday.

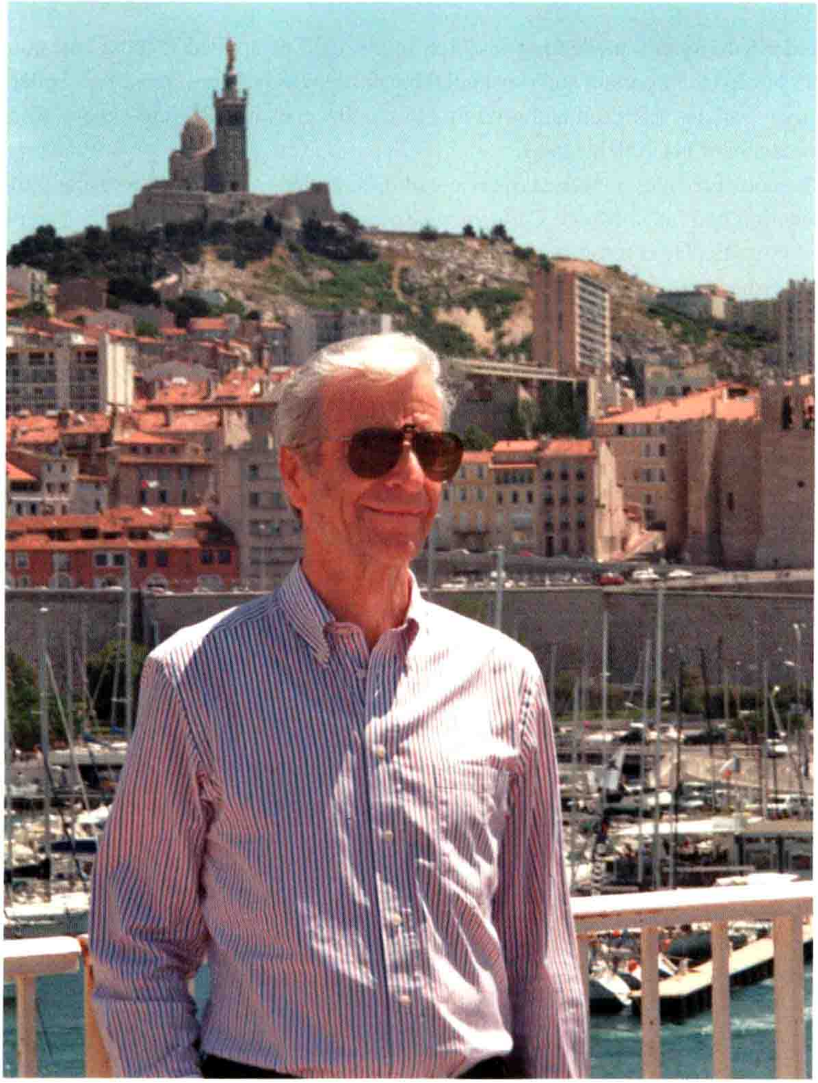
The book provides a modern overview of different research areas, covering uniform distribution and quasi-Monte Carlo methods as well as finite fields and their applications, in particular cryptography and pseudorandom number generation. Many results are published here for the first time. The book serves as a useful starting point for graduate students new to these areas, or as a refresher for researchers wanting to follow recent trends.

GERHARD LARCHER is Full Professor for Financial Mathematics and Head of the Institute for Financial Mathematics at the Johannes Kepler University Linz.

FRIEDRICH PILLICHSHAMMER is Associate Professor in the Institute for Financial Mathematics at the Johannes Kepler University Linz.

ARNE WINTERHOF is Senior Fellow at the Johann Radon Institute for Computational and Applied Mathematics (RICAM) at the Austrian Academy of Sciences, Linz.

CHAOPING XING is Full Professor in the Department of Physical and Mathematical Sciences at Nanyang Technological University, Singapore.



Harald Niederreiter in Marseille, 2013

Preface

Harald Niederreiter's pioneering research in the field of applied algebra and number theory has led to important and substantial breakthroughs in many areas, including finite fields and areas of their application such as coding theory and cryptography as well as uniform distribution and quasi-Monte Carlo methods. He is the author of more than 350 research papers and 10 books.

This book contains essays from close colleagues and leading experts in those fields in which he has worked. The essays contain short overviews of different research areas as well as some very new research results.

The articles focus on uniform distribution and quasi-Monte Carlo methods as well as finite fields and their applications, in particular cryptography and pseudorandom number generation.

The first chapter gives an overview of Harald's career and describes some scientific spotlights.

Linz and Singapore, January 2014
Gerhard Larcher, Friedrich Pillichshammer,
Arne Winterhof and Chaoping Xing

Contents

The color plates are situated between pages 294 and 295.

1
Some highlights of Harald Niederreiter's work

Gerhard Larcher and Friedrich Pillichshammer
Johannes Kepler University Linz

Arne Winterhof
Austrian Acadamy of Sciences, Linz

Chaoping Xing
Nanyang Techological University, Singapore

Dedicated to our teacher, colleague and friend, Harald Niederreiter, on the occasion of his 70th birthday.

Abstract

In this paper we give a short biography of Harald Niederreiter and we spotlight some cornerstones from his wide-ranging work. We focus on his results on uniform distribution, algebraic curves, polynomials and quasi-Monte Carlo methods. In the flavor of Harald's work we also mention some applications including numerical integration, coding theory and cryptography.

1.1 A short biography

Harald Niederreiter was born in Vienna in 1944 on June 7 and spent his childhood in Salzburg. In 1963 he returned to Vienna to study at the Department of Mathematics of the University of Vienna, where he finished his PhD thesis entitled "Discrepancy in compact Abelian groups" *sub auspiciis praesidentis rei publicae*[1] under the supervision of Edmund Hlawka in 1969. From 1969 to 1978 he worked as scientist and professor in the USA at four different institutes: Southern Illinois University, University of Illinois at Urbana-Champaign, Institute for Advanced Study, Princeton, and University of California at Los Angeles. From 1978 to 1981 he was Chair of Pure Mathematics at the University of the West Indies in Kingston (Jamaica). He

[1] The term "Promotion sub auspiciis praesidentis rei publicae" is the highest possible honor for course achievement at school and university in Austria.

returned to Austria and served as director of two institutes of the Austrian Academy of Sciences in Vienna, of the Institute for Information Processing until 1999 and then of the Institute of Discrete Mathematics. From 2001 to 2009 he was professor at the National University of Singapore. Since 2009 he has been located at the Johann Radon Institute for Computational and Applied Mathematics in Linz. From 2010 to 2011 he was professor at the King Fahd University of Petroleum and Minerals in Dhahran (Saudi Arabia).

Harald Niederreiter's research areas include numerical analysis, pseudorandom number generation, quasi-Monte Carlo methods, cryptology, finite fields, applied algebra, algorithms, number theory and coding theory. He has published more than 350 research papers and several books, including the following.

- (with L. Kuipers) *Uniform Distribution of Sequences*. Wiley-Interscience, 1974; reprint, Dover Publications, 2006.
- (with R. Lidl) *Finite Fields*. Encyclopaedia of Mathematics and its Applications, volume 20. Addison-Wesley, 1983; second edition, Cambridge University Press, 1997.
- (with R. Lidl) *Introduction to Finite Fields and their Applications*. Cambridge University Press, 1986; revised edition, 1994.
- *Random Number Generation and Quasi-Monte Carlo Methods*. CBMS-NSF Regional Conference Series in Applied Mathematics, volume 63. Society for Industrial and Applied Mathematics (SIAM), 1992.
- (with C. P. Xing) *Rational Points on Curves over Finite Fields: Theory and Applications*. London Mathematical Society Lecture Note Series, volume 285. Cambridge University Press, 2001.
- (with C. P. Xing) *Algebraic Geometry in Coding Theory and Cryptography*. Princeton University Press, 2009.

Furthermore he is editor or co-editor of the following proceedings.

- (with P. J.-S. Shiue) *Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing*. Springer-Verlag, 1995.
- (with S. D. Cohen) *Finite Fields and Applications*. London Mathematical Society Lecture Note Series, volume 233. Cambridge University Press, 1996.
- (with P. Hellekalek, G. Larcher and P. Zinterhof) *Monte Carlo and Quasi-Monte Carlo Methods 1996*. Springer-Verlag, 1998.
- (with C. Ding and T. Helleseth) *Sequences and their Applications*. Springer-Verlag, 1999.

- (with J. Spanier) *Monte Carlo and Quasi-Monte Carlo Methods 1998*. Springer-Verlag, 2000.
- (with D. Jungnickel) *Finite Fields and Applications*. Springer-Verlag, 2001.
- (with K.-T. Fang and F. J. Hickernell) *Monte Carlo and Quasi-Monte Carlo Methods 2000*. Springer-Verlag, 2002.
- *Coding Theory and Cryptology*. World Scientific, 2002.
- *Monte Carlo and Quasi-Monte Carlo Methods 2002*. Springer-Verlag, 2004.
- (with K. Feng und C. P. Xing) *Coding, Cryptography and Combinatorics*. Birkhäuser-Verlag, 2004.
- (with D. Talay) *Monte Carlo and Quasi-Monte Carlo Methods 2004*. Springer-Verlag, 2006.
- (with A. Keller and S. Heinrich) *Monte Carlo and Quasi-Monte Carlo Methods 2006*. Springer-Verlag, 2008.
- (with Y. Li, S. Ling, H. Wang, C. P. Xing and S. Zhang) *Coding and Cryptology*. World Scientific, 2008.
- (with A. Ostafe, D. Panario and A. Winterhof) *Algebraic Curves and Finite Fields: Cryptography and Other Applications*. de Gruyter, 2014.
- (with P. Kritzer, F. Pillichshammer and A. Winterhof) *Uniform Distribution and Quasi-Monte Carlo Methods: Discrepancy, Integration and Applications*. de Gruyter, 2014.

Some important methods are named after him, such as the Niederreiter public-key cryptosystem, the Niederreiter factoring algorithm for polynomials over finite fields, and the Niederreiter and Niederreiter–Xing low-discrepancy sequences.

Some of his honors and awards are

- full member of the Austrian Academy of Sciences
- full member and former member of the presidium of the German Academy of Natural Sciences Leopoldina
- Cardinal Innitzer Prize for Natural Sciences in Austria
- invited speaker at ICM 1998 (Berlin) and ICIAM 2003 (Sydney)
- Singapore National Science Award 2003
- honorary member of the Austrian Mathematical Society 2012
- Fellow of the American Mathematical Society 2013.

Niederreiter was also the initiator and, from 1994 to 2006, the co-chair of the first seven biennial *Monte Carlo and quasi-Monte Carlo meetings* which took place in

- Las Vegas, NV, USA (1994)
- Salzburg, Austria (1996)

- Claremont, CA, USA (1998)
- Hong Kong (2000)
- Singapore (2002)
- Juan-Les-Pins, France (2004)
- Ulm, Germany (2006)
- Montreal, Canada (2008)
- Warsaw, Poland (2010)
- Sydney, Australia (2012)
- Leuven, Belgium (2014).

In 2006 Harald Niederreiter announced his wish to step down from the organizational role, and a Steering Committee was formed to ensure and oversee the continuation of the conference series.

1.2 Uniform distribution theory and number theory

When we scroll over the more than 350 scientific articles by Niederreiter which have appeared in renowned journals such as *Mathematika*, *Duke Mathematical Journal*, *Bulletin of the American Mathematical Society* and *Compositio Mathematica*, we find that most of these papers have connections to topics from number theory or use techniques from number theory, and many of the articles deal with problems and solve open questions, or initiate a new field of research in the theory of uniform distribution of sequences. The later sections in this overview of Harald's work on coding theory, algebraic curves and function fields, pseudorandom numbers, finite fields, and quasi-Monte Carlo methods in a certain sense will also deal with number-theoretical aspects.

Let us give just one example: the analysis and the precise estimation of exponential sums $\sum_{k=0}^{N-1} \mathrm{e}^{2\pi \mathrm{i} f(k)}$ or, in particular, of character sums plays an essential role in many different branches of mathematics and especially in number theory. In particular, it plays a basic role in many questions concerning uniform distribution of sequences, discrepancy theory, quasi-Monte Carlo methods, pseudorandom number analysis, the theory of finite fields, and many more. In a variety of papers on exponential sums and their applications, Niederreiter has proven to be a leading expert in the analysis of exponential sums and has essentially developed a variety of important techniques.

In this section we want to pick out some of the most impressive of Niederreiter's work on topics in number theory and in uniform distribution theory that will not be described explicitly in subsequent sections.

In the first years after finishing his PhD thesis "Discrepancy in compact Abelian groups" under the supervision of Edmund Hlawka, Niederreiter was