Lecture Notes in Computer Science 1838
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Wieb Bosma (Ed.)

Algorithmic Number Theory

4th International Symposium, ANTS-IV
Leiden, The Netherlands, July 2-7, 2000
Proceedings

Wieb Bosma
University of Nijmegen, Mathematical Institute
Postbus 9010, 6500 GL Nijmegen, The Netherlands
E-mail: bosma@sci.kun.nl

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Algorithmic number theory : 4th international symposium ; proceedings / ANTS-IV, Leiden, The Netherlands, July 2 - 7, 2000. Wieb Bosma (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2000
(Lecture notes in computer science ; Vol. 1838)
ISBN 3-540-67695-3

CR Subject Classification (1998): I.1, F.2.2, G.2, E.3-4, J.2

ISSN 0302-9743
ISBN 3-540-67695-3 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Christian Grosche, Hamburg
Printed on acid-free paper SPIN: 10722028 06/3142 5 4 3 2 1 0

Preface

The fourth Algorithmic Number Theory Symposium takes place at the Universiteit Leiden, in the Netherlands, from July 2-7, 2000. Its organization is a joint effort of Dutch number theorists from Leiden, Groningen, Nijmegen, and Amsterdam.

Six invited talks and 36 contributed talks are scheduled. This volume contains the written versions of the talks, with the exception of two of the invited talks. Not included are: *A rational approach to* π by Frits Beukers (Utrecht) and *The 40 trillionth binary digit of* π *is* 0 by Peter Borwein (Burnaby, Canada). These talks are aimed at a wider audience, and form part of the special ANTS IV event *Pi in de Pieterskerk* on July 5, 2000. This event includes an evening ceremony in which the tombstone of Ludolph van Ceulen is replaced. Van Ceulen, who was appointed to Leiden in 1600, calculated 35 decimals of π. His tombstone in the Pieterskerk, in which these decimals were engraved, disappeared in the 19th century.

ANTS in Leiden is the fourth in a series of symposia that started in 1994. Previous locations were Cornell University, Ithaca, New York (1994), Université de Bordeaux I in Bordeaux, France (1996), and Reed College, Portland, Oregon (1998). The diversity of the papers contained in this volume shows that the main theme of ANTS, algorithmic number theory, is taken in a broad sense. The number of submissions for the Leiden conference largely exceeded the physical limitations of our one-week schedule. We are therefore confident that we are only at the beginning of a continuing tradition.

May 2000

Peter Stevenhagen
ANTS IV Program Chair
Wieb Bosma
Proceedings Editor

Organization

Organizing Committee

Wieb Bosma (Katholieke Universiteit Nijmegen)
Herman te Riele (CWI, Amsterdam)
Bart de Smit (Universiteit Leiden)
Peter Stevenhagen (Universiteit Leiden)
Jaap Top (Rijksuniversiteit Groningen)

Advisory Board

Dan Boneh (Stanford University)
Joe P. Buhler (Reed College, Portland)
Arjen K. Lenstra (Citibank)
Hendrik W. Lenstra, Jr. (UC Berkeley, and Universiteit Leiden)
Andrew M. Odlyzko (AT&T)
Rob Tijdeman (Universiteit Leiden)

Sponsoring Institutions

The organizers of ANTS IV gratefully acknowledge financial support from the following organizations.

Beegerfonds, CWI
Centrum voor Wiskunde en Informatica
Koninklijke Nederlandse Akademie van Wetenschappen
Lorentz Center
Mathematical Research Institute
Rekenkamer Ludolph van Ceulen
Thomas Stieltjes Institute for Mathematics
Universiteit Leiden

Table of Contents

Invited Talks

Contributed Papers